Explicit Serre weights for two-dimensional Galois representations

Steinmetz, Misja Frederik Alban

Awarding institution:
King's College London

Explicit Serre weights for two-dimensional Galois representations

Misja Frederik Alban Steinmetz

Supervisor: Prof. Fred Irvin Diamond
Second Supervisor: Prof. Kevin Mark Buzzard

Submitted for the degree of Doctor of Philosophy
Department of Mathematics
King's College London

August 2019

ABSTRACT

Let F be a totally real field and p a prime number. Given a Galois representation $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$, we have precise conjectures (see [BLGG13]) in terms of non-explicit p-adic Hodge theory giving the sets of weights of Hilbert modular forms such that the reduction of the associated Galois representation is isomorphic to ρ. Under the assumption that p is unramified in F an alternative explicit formulation of these sets of weights was proposed in the paper [DDR16] replacing the p-adic Hodge theory by local class field theory. Subsequently, the equivalence of the reformulated conjecture to the original conjecture was proved in [CEGM17].

In this thesis we generalise the conjecture of [DDR16] and the proof of equivalence of the two conjectures of [CEGM17] to hold for any totally real field F. Thereby, we give an equivalent explicit version of the conjectures on the modularity of two-dimensional Galois representations over totally real fields.

Contents

CHAPTER 1

Introduction

For a totally real field F, a prime p and a mod p Galois representation $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$, the question whether this representation can arise as the reduction of the Galois representation associated to a Hilbert modular form was first rigorously studied in [BDJ10] under the hypothesis that p is unramfied in F. This being a generalisation of Serre's famous conjecture [Ser87] for $F = \mathbf{Q}$, it was long believed that a similar conjecture could be formulated for totally real fields. However, in the conjecture of [BDJ10], the authors were for the first time able to predict the set of weights of Hilbert modular forms leading to the given representation precisely. The unramifiedness hypothesis was later removed in Schein [Sch08], [Gee11] and [BLGG13]. Building on previous work of Gee and co-authors it was proved in [GLS15] that the predicted set of weights of [BDJ10] and its extensions is correct in the sense that if ρ comes from a Hilbert modular form then it must come from a form of weight predicted by the conjectures and every predicted weight occurs.

One unifying aspect of all these conjectures is that the sets of weights are predicted using abstract p-adic Hodge theory making it complicated to do explicit computations in many cases. This problem was addressed in the paper [DDR16] under the assumption that p is unramified in F. The authors conjecture an alternative explicit formulation of the predicted sets of weights in terms of local class field theory and the Artin–Hasse exponential. Subsequently, it was proved in [CEGM17] that their reformulation was equivalent to the original conjectures. The main result of this thesis is the generalisation of the conjecture of [DDR16] as well as a a generalisation of the proof of the equivalence of the two conjectures of [CEGM17] to the case of an arbitrary totally real field F. As an immediate consequence, we can give an alternative, explicit and equivalent formulation of the sets of weights appearing in the conjectures on the modularity of two-dimensional mod p Galois representations over an arbitrary totally real field.

Let us now give a more careful chapter-by-chapter overview of the contents of this thesis. In Chapter 2 and 3 we give some history and background in order to put the results of this thesis in a broader context. In

Chapter 2 we describe Serre's modularity conjecture on Galois representation $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ through some of the original letters between Serre, Tate and Grothendieck. We move on to give a cohomological reformulation of the weight part of Serre's conjecture in which we use the Eichler–Shimura isomorphism to redefine ρ being modular in terms of the non-vanishing to localisations of certain group cohomology groups. Lastly, we will explain how this cohomological formulation is related to crystalline lifts of $\rho|_{G_{\mathbf{Q}_p}}$ of certain prescribed Hodge–Tate weights. These reformulations are important for the generalisations of Serre's conjecture treated in the following chapter.

In Chapter 3 we introduce generalisations of Serre's modularity conjecture to Galois representations $\rho\colon \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ for a totally real field F. We start with a very brief introduction to the theory of Hilbert modular forms. Next we sketch how to define modularity of Galois representations in this context following [BDJ10, §2]. To define the associated sets of weights $W(\rho)$ we restrict to a decomposition group at a prime $\mathfrak{p}$ of F dividing p. Writing $\rho_{\mathfrak{p}}$ for the resulting local representation at this prime, we define $W(\rho_{\mathfrak{p}})$ explicitly if $\rho_{\mathfrak{p}}$ is irreducible. The reducible case requires more attention. Suppose

$$\rho_{\mathfrak{p}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

for continuous characters $\chi_1, \chi_2\colon G_{F_{\mathfrak{p}}} \to \overline{\mathbf{F}}_p^{\times}$. Then $\rho_{\mathfrak{p}}$ defines a cocycle in the space of extensions $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ of $\overline{\mathbf{F}}_p(\chi_2)$ by $\overline{\mathbf{F}}_p(\chi_1)$, where $\chi := \chi_1\chi_2^{-1}$. We include a weight V in $W(\rho_{\mathfrak{p}})$ if and only if this associated cocycle lies in a mysterious subspace $L_V \subseteq H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ depending on the weight V. At the end of the chapter we give a definition of the subspaces L_V in terms of the existence of crystalline lifts of certain prescribed Hodge–Tate weights. All this results a precise statement of the generalisation of Serre's conjecture to two dimensional mod p Galois representations of totally real fields.

In Chapter 4 we prove a result that seems to be well-known to experts, but for which we have been unable to find an appropriate reference. If χ is the cyclotomic character, then we can use Kummer theory to identify $H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \cong K^\times \otimes \overline{\mathbf{F}}_p$. The *peu ramifié* subspace is the subspace of cocycles corresponding to elements of the codimension-one subspace $\mathcal{O}_K^\times \otimes \overline{\mathbf{F}}_p$. The result we prove in this chapter is that the subspaces $L_V \subseteq H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ are contained in the peu ramifié subspace (except in one exceptional case). We prove this by first proving the result in the trivial weight case using the theory of finite flat group schemes. Then we prove that we have inclusions $L_V \subseteq L_{V_{\mathrm{triv}}}$ using the classification of [GLS15]. In the hope of making this chapter useful without the need to read the rest of the thesis, we have tried to keep it somewhat self-contained.

In Chapter 5 we define an explicit basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ by making use of local class field theory and the Artin–Hasse exponential. That is, we generalise [DDR16, §3,§5] to the case of an arbitrary local field K. We start by defining a filtration on $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ via restrictions to higher ramification groups and we find the jumps of this filtration as well as their dimension. Then we study the dual filtration which is defined using local class field theory and given in terms of the higher unit groups of a tamely ramified extension of K. Using the Artin–Hasse exponential we define basis elements $\{u_{i,j}\}$ in these higher unit groups and we obtain a basis $\{c_{i,j}\}$ of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ dually.

In Chapter 6 we study the relationship between the explicitly defined basis elements of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ from the previous chapter and the spaces L_V defined using crystalline lifts. This is a generalisation of [CEGM17, §3] to the case of an arbitrary local field K. We start by recalling some p-adic Hodge theory as well as the classification theorem of [GLS15] which classifies the space L_V in terms of the étale φ-modules that it corresponds to. Via Artin–Schreier theory and the theory of the field of norms, we use an explicit reciprocity law to write down a precise criterion for when the pairing of (the image of) L_V with $u_{i,j}$ does not vanish. Writing J_V^{AH} for the pairs (i,j) satisfying this criterion, we then conclude that the span of $L_V^{\mathrm{AH}} := \{c_{i,j} \mid (i,j) \in J_V^{\mathrm{AH}}\}$ must equal L_V. This gives an alternative explicit way of writing down the subspaces L_V. We remark that special cases of Chapters 5 and 6 are related to Abrashkin's papers [Abr89] and [Abr97]. The first paper implies cases of our conjecture and in the second paper the Artin–Hasse exponential appears much like in our work.

In Chapter 7 we study the criterion in the defintion of J_V^{AH} in some more detail. We start with generalisations of [DDR16, §4,§6]. That is, we introduce the concept of dependency which gives us a direct condition that the spaces L_V^{AH} should satisfy if they are independent of some choices made in their definition. Of course, at this point we have already proved that $L_V = L_V^{\mathrm{AH}}$ from which it follows, a posteriori, that the latter space is choice-independent. However, we will see that the concept of dependency will make it easier to write down an explicit formula for the elements of the set J_V^{AH}. We move on by recalling from [DDR16] what such a formula looks like in the case that K is unramified over $\mathbf{Q}_p$. We recall that a combinatorial proof of the correctness of this formula is given in [CEGM17]. Next we turn to the case that K is a totally ramified extension of $\mathbf{Q}_p$. We give an explicit formula in this case and prove that this indeed gives the set J_V^{AH}. At the end of the chapter we look at the two special cases when χ is *generic* or when $e = 2$ and we give conjectural formulae for the elements of the set J_V^{AH} in these cases. It would have been nice to be able to find a more explicit formula for the elements of the set J_V^{AH} in complete generality, however the combinatorics of the problem become quite difficult fairly quickly. More work needs to be done to solve this problem in general.

1.1. Notation

In this thesis the number p will always denote a prime. For any field F we will write $G_F := \mathrm{Gal}(\overline{F}/F)$ for the absolute Galois group of F. If we let F be a finite extension of $\mathbf{Q}$ and $\mathfrak{p}$ a prime ideal, we will write $F_{\mathfrak{p}}$ for the completion of F at the given prime ideal. Once and for all we will fix embeddings $\overline{F} \hookrightarrow \mathbb{C}$ and $\overline{F} \hookrightarrow \overline{F}_{\mathfrak{p}}$. This gives a natural sequence of subgroups

$$I_{F_{\mathfrak{p}}} \subset G_{F_{\mathfrak{p}}} := \mathrm{Gal}(\overline{F}_{\mathfrak{p}}/F_{\mathfrak{p}}) \subset G_F := \mathrm{Gal}(\overline{F}/F),$$

where $I_{F_{\mathfrak{p}}}$ denotes the inertia group at $\mathfrak{p}$. When dealing directly with finite extensions K of $\mathbf{Q}_p$ we let $I_K \subset G_K$ have the same meaning as in the completed global case.

We will write ε for the p-adic cyclotomic character $\varepsilon : G_K \to \mathbf{Z}_p^\times$ of K defined by $\sigma(\zeta) = \zeta^{\varepsilon(\sigma)}$ for any $\sigma \in G_K$ and any compatible sequence of higher pth roots of unity $\zeta \in \mu_{p^\infty}(\overline{K})$. In situations where it is important to distinguish the characteristic zero theory from the characteristic p theory, we will write $\overline{\varepsilon} : G_K \to \mathbf{F}_p^\times$ for the reduction mod p of ε. When the distinction is clear from context we will, by abuse of notation, sometimes also write ε for the reduction mod p.

We let $K/\mathbf{Q}_p$ be a finite extension of ramification index e, of residue degree f and with residue field k. We fix an embedding $\overline{\tau}_0 \in \mathrm{Hom}(k, \overline{\mathbf{F}}_p)$ and label the remaining embeddings of the residue field via the rule $\overline{\tau}_{i+1}^p = \overline{\tau}_i$. This is the convention as in [GLS15], opposite to [DDR16]. We now label the embeddings

$$\mathrm{Hom}(K, \overline{\mathbf{Q}}_p) = \{\tau_{i,j} \mid i = 0, \ldots, f-1 \ , \ j = 0, \ldots, e-1\}$$

in any way such that $\tau_{i,j} \equiv \overline{\tau}_i \bmod p$. When it is convenient we may consider the indices of the embeddings to be elements of $\mathbf{Z}/f\mathbf{Z}$ and $\mathbf{Z}/f\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}$, meaning, for example, that $\overline{\tau}_f = \overline{\tau}_0$ and $\tau_{f,e} = \tau_{0,0}$ etcetera. Let G_K denote the absolute Galois group of K and fix a uniformiser π_K of K. We set $\pi_0 := \pi_K$ and for each $n \geqslant 1$ we choose a p^n-th root of π_K such that $\pi_{n+1}^p = \pi_n$. We define the rising union $K_\infty := \bigcup_{n\geqslant 0} K(\pi_n)$; when $p = 2$ we will furthermore suppose that π_K was chosen so that $K_\infty \cap K_{p^\infty} = K$, where $K_{p^\infty} := \bigcup_{n\geqslant 1} K(\zeta_{p^n})$ with ζ_{p^n} a primitive p^n-th root of unity – it follows from [Wan17, Lem. 2.1] that this is always possible. For any unramified extension L of K we let $\mathrm{Frob}_K \in \mathrm{Gal}(L/K)$ denote the arithmetic Frobenius.

Let π be a root of $x^{p^f-1} + \pi_K$ in $\overline{K}$. Recall that we have a character $\overline{\omega}_\pi : G_K \to k^\times$ defined by

$$\sigma \mapsto \frac{\sigma(\pi)}{\pi} \bmod \pi_K.$$

For any embedding $\overline{\tau} \in \mathrm{Hom}(k, \overline{\mathbf{F}}_p)$ we get a **fundamental character** $\omega_{\overline{\tau}} : G_K \to \overline{\mathbf{F}}_p^\times$ via $\omega_{\overline{\tau}} := \overline{\tau} \circ \overline{\omega}_\pi$. When $\overline{\tau} = \overline{\tau}_i$ this character is also sometimes simply denoted by ω_i. The characters $\{\omega_i \mid i = 0, \dots, f-1\}$ are often called the fundamental characters of level f.

1.2. Conventions in p-adic Hodge theory

In this thesis we will not give an extensive background treatment of the theory of p-adic Hodge theory despite it being used extensively in Chapters 2, 3 and, most importantly, in Chapter 6. A good survey of the fundamentals of p-adic Hodge theory would require a substantial amount of space. Moreover, very good surveys are available already such as the excellent short survey [Ber04] and the fine longer and more detailed survey [BC09]. Therefore, we have chosen to put the focus of the background material of this thesis on arguments that we believe to be less easily found in the literature. Nonetheless, let us give an hypercondensed overview of the material here, mainly to fix our conventions. For more details, we refer to the surveys [Ber04] and [BC09].

1.2.1. Crystalline Representations. Let K be a p-adic local field. In the 1980s Fontaine introduced the period ring B_{dR}, which is a filtered K-algebra endowed with a G_K-action, and its subring B_{cris} on which one can define a natural Frobenius map (see [Ber04, §II.2,§II.3] for the exact definitions). If V is an n-dimensional $\overline{\mathbf{Q}}_p$-vector space and $\rho : G_K \to \mathrm{GL}(V)$ a representation. Then we will say ρ is **de Rham** (resp. **crystalline**) if $(B \otimes_{\mathbf{Q}_p} V)^{G_K}$ is a free module over $K \otimes_{\mathbf{Q}_p} \overline{\mathbf{Q}}_p$ (resp. $K_0 \otimes_{\mathbf{Q}_p} \overline{\mathbf{Q}}_p$) of rank n for $B = B_{\mathrm{dR}}$ (resp. $B = B_{\mathrm{cris}}$), where G_K acts diagonally on the tensor product. It turns out that any crystalline representation is also de Rham.

Some intuition for this definition can be given as follows. Suppose E is an elliptic curve defined over $\mathbf{Q}_p$. For any prime ℓ we can look at its ℓ-adic Tate module $T_\ell E := \varprojlim_n E[\ell^n](\overline{\mathbf{Q}}_p)$ on which $G_{\mathbf{Q}_p} := \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ acts naturally. We may wonder whether it is possible to determine whether E has good reduction at p simply from studying the properties of the representation $\rho_E : G_{\mathbf{Q}_p} \to \mathrm{GL}_2(\overline{\mathbf{Q}}_\ell)$ obtained from this action. Indeed, if $p \neq \ell$ the criterion of Néron, Ogg and Shafarevich says that E has good reduction at p if and only if this representation is unramified. When $\ell = p$, however, the condition of unramifiedness does not work any longer and needs to be replaced by the condition that the representation is crystalline. Therefore, one (vague) way of thinking about crystalline representations is as representations $G_{\mathbf{Q}_p} \to \mathrm{GL}_n(\overline{\mathbf{Q}}_p)$ coming from geometric objects over $\mathbf{Q}_p$ with good reduction at p.

1.2.2. Hodge–Tate weights. Let $\widehat{\overline{K}}$ be the completion of the algebraic closure $\overline{K}$ of K. For an integer i, we write $\widehat{\overline{K}}(i)$ for the i-th **Tate twist** of this vector space, i.e. the same underlying vector space with the action of G_K given by the i-th power of the p-adic cyclotomic character. Given a crystalline (hence de Rham) representation $\rho\colon G_{\mathbf{Q}_p} \to \mathrm{GL}(V)$, we define its Hodge–Tate weights as follows: for $\tau \in \mathrm{Hom}(K, \overline{\mathbf{Q}}_p)$ we define the τ-**labelled Hodge–Tate weights** $\mathrm{HT}_\tau(\rho)$ of ρ to be the multiset of integers containing the integer i with multiplicity

$$\dim_{\overline{\mathbf{Q}}_p}(V \otimes_{\tau,K} \widehat{\overline{K}}(-i))^{G_K}$$

with Galois acting diagonally. It follows from the definition that the p-adic cyclotomic character ε has Hodge–Tate weight 1. If you prefer geometry, then another way of thinking about this is the following. If X is a proper scheme over $\mathbf{Q}_p$ with good reduction at p, then the Hodge–Tate weights of $H^i_{\text{ét}}(X_{\overline{\mathbf{Q}}_p}, \overline{\mathbf{Q}}_p)$ (as a $G_{\mathbf{Q}_p}$-representation) are simply the jumps (with multiplicity) in the filtration on the de Rham cohomology.

1.3. Acknowledgements

First and foremost I would like to thank my supervisor, Fred Diamond, for his support during the past four years. Fred's mathematical contributions to this thesis are innumerable: from small encouragements to try to pursue a certain approach, which often turned out to be invaluable, to long explanations of complicated arguments. Many of the results of this thesis would not have existed if it wasn't for Fred's suggestions and explanations. At times when I was stuck, I found Fred's firm belief in positive reinforcement and his calm kind supervising style helpful and encouraging. Therefore, let me thank him wholeheartedly for his guidance throughout this process in the last four years.

I would like to thank Dougal Davis, who was unfortunate enough to be assigned the desk next to me, for answering even the silliest of my questions and Robin Bartlett for basically single-handedly teaching me p-adic Hodge theory. I would also like to thank Toby Gee, Esther Polak, Ashwin Iyengar, James Newton, Victor Abrashkin, Pol van Hoften and Laurent Berger for helpful mathematical conversations and suggestions. Furthermore, I would like to thank the remaining students from my King's office, Sebastian Lautz, Hanneke Wiersema and Sarah Nowell, for keeping the atmosphere at the office just high enough that it was ever so slightly more enjoyable to work from the office than alone at home (and for their appreciation of sarcastic comments).

On a more personal note, I would like to thank my parents, Carl and Erica, without whose continued love, support and rock-solid belief, often through difficult times, it is hard to imagine things would have worked out as well as they did. I would like to thank my sisters, Tisha and Esther, who are always there when you need them, my stepmother and stepsisters, Ruth, Niki and Ruby, and my dear longtime friend, Xander, for their support in these years. Of course, I would also like to thank my girlfriend Camilla, whose love, kindness as well as a no-nonsense can-do approach were a huge help at times when it was needed most. Certainly Camilla's proofreading abilities also came in handy in the preparation of the final version of this thesis. Lastly, let me mention those people that unfortunately are not here anymore to witness the completion of this thesis, but whose influence will never fade: Caro, Daan, Oma Vonne and Carlo.

This work was supported by the Engineering and Physical Sciences Research Council [EP/L015234/1]. During the research the author was a registered student at The EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College London. During this time the author was also registered as a student at the Department of Mathematics, King's College London, and could often be found at Imperial College London (who were kind enough to provide him with a workspace). In addition from February until April of 2019 the author was a visiting researcher at the Mathematical Institute of Leiden University in the Netherlands. The author would like to thank all the institutions above for their support and hospitality.

CHAPTER 2

The weight in Serre's conjecture

In this chapter we will take a historical look at Serre's conjecture. We will explain how to 'geometrise' the weight in the conjecture: a reformulation of the weight part of Serre's conjecture will prove to be of vital importance for generalisations of his conjecture in following chapters. We stress that this chapter is provided as an introduction and motivation to the topics that will come later in this thesis and none of the work presented here is originally due to the author. We found the introduction of [GHS18] and Florian Herzig's talk [Her10] at the Institute of Advanced Study in Princeton helpful in our preparation of this chapter.

2.1. Historical notes on Serre's conjecture

The history of the area of number theory that this thesis is a part of, which is nowadays often referred to as the 'Serre weight conjectures', all starts with a conjecture made by Jean-Pierre Serre in 1973 in a letter to John Tate [ST15, p.451]. The details were worked out by Serre in the following decade and a half until he published a precise form of his conjecture in 1987 [Ser87]. In his letter of the first of May 1973, Jean–Pierre Serre writes the following to John Tate (quoted from [ST15, pp. 451–453]; translation by the author).

> Dear Tate,
>
> [...] I would like to tell you about a conjecture on Galois extensions of $\mathbf{Q}$ whose Galois group is a subgroup of $\mathrm{GL}_2(\mathbf{F}_p)$:
>
> I will be careful, and consider only representations
>
> $$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_q), \qquad q = p^f,$$
>
> unramified outside of p and satisfying the following condition:
>
> $$\det \rho : \mathrm{Gal} \to \mathbf{F}_q^* \text{ is equal to } \chi^{k-1} \quad (k \text{ even}),$$

where $\chi : \mathrm{Gal} \to \mathbf{F}_q^*$ is the fundamental character modulo p (given by the action on $\boldsymbol{\mu}_p$).

In fact, this condition is equivalent to: the image under ρ of the real Frobenius has eigenvalues $+1$ and -1 (*i.e.*, $\det \rho$ is an *odd* character).

[...] If $\ell \neq p$, the trace and determinant of $\rho(\mathrm{Frob}_\ell)$ have an obvious meaning; denote them by a_ℓ and l^{k-1}, and take the Dirichlet series (with coefficients in $\mathbf{F}_q$)

$$\prod_{\ell \neq p} (1 - a_\ell l^{-s} + \ell^{k-1-2s})^{-1},$$

à la Hecke; denote it by $\sum a_n n^{-s}$, and take the formal series

$$f = \sum_{n=1}^{+\infty} a_n q^n,$$

where this time q denotes a variable... a thousand apologies for having used q for the number of elements of the finite field, but I'm too lazy to start over for so little!

Conjecture. *The series f is a modular form (modulo p) for $\mathrm{SL}_2(\mathbf{Z})$ of weight congruent to k* mod $(p-1)$.

[...] Enough talking like so. Until another time.

J.-P. Serre

Let us briefly explain what Serre is proposing in his letter. Since the 1971 paper of Deligne [Del71] it was known that starting with a eigenform f of weight $k \geqslant 2$, level $\Gamma_1(N)$ and character χ it was possible to attach to f a continuous irreducible p-adic representation $\rho_f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$. The modular form defines the representation uniquely: ρ_f is unramified at any $\ell \nmid Np$ and $\rho_f(\mathrm{Frob}_\ell)$ has characteristic polynomial $x^2 - a_\ell(f)t + \chi(\ell)\ell^{k-1}$.

What Serre describes in his letter is a mod p analogue of this result going the other way, that is, starting with a mod p Galois representation he would like to obtain a mod p modular form. One way of stating the question is as follows. It is not hard to show that the representation ρ_f will always fix a lattice, and we can reduce the representation acting on the lattice $\rho_f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{Z}}_p)$ modulo p. If we do not want our reduced representation to depend on the choice of lattice, we have to semisimplify the mod p representation after the reduction. Then we have attached a (continuous) mod p representation $\overline{\rho}_f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ to our eigenform f. The connection between the modular form and the mod p Galois representation is then characterised by $\mathrm{Tr}\,\overline{\rho}_f(\mathrm{Frob}_\ell) = \overline{a_\ell(f)}$ and $\det \overline{\rho}_f(\mathrm{Frob}_\ell) = \overline{\chi(\ell)l^{k-1}}$.

One simplistic way of thinking about modular forms modulo p is simply as reductions of q-expansions of characteristic 0 modular forms, so by the process above we have indeed found a way of attaching a mod p Galois representation to a mod p modular form. Serre would like to go the other way. Because he is being careful he is restricting himself to modular forms of level $\Gamma_1(1)$ with χ trivial, that is, modular forms for $\mathrm{SL}_2(\mathbf{Z})$. Suppose we are given a mod p representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_q)$ for $q = p^f$. Under mild additional hypotheses on $\overline{\rho}$, namely that $\overline{\rho}$ is unramified outside of p and $\det \overline{\rho}$ is equal to $\overline{\varepsilon}^{k-1}$ for the mod p cyclotomic character $\overline{\varepsilon}$, Serre conjectures in his letter to Tate above that $\overline{\rho}$ must always arise from a modular form. In this case that comes down to the claim that for any such $\overline{\rho}$ there exists a characteristic 0 modular form f for $\mathrm{SL}_2(\mathbf{Z})$ such that for all primes $\ell \neq p$ we have that $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_\ell) = \overline{a_\ell(f)}$.

The conjecture that Serre makes in the above letter to Tate is quite remarkable. This can also be seen from the enthusiastic reactions of Tate in following letters.

> "Dear Serre, your conjecture (or question if you want to be chicken) about modular representations of degree 2 of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and modular forms is beautiful!" – John Tate, 11th of June 1973 [ST15, p. 456].

> "Dear Serre, please give me a little more time [...] on the elliptic curve report. I *have* started it, but have been distracted by various things, in particular, your conjectures on $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_{\ell^a})$." – John Tate, 2nd of July 1973 [ST15, p. 462].

Serre spends a good part of the next decade and a half generalising and refining his conjecture. The first sought after generalisation is to allow for modular forms of a general weight k and level N. This poses a problem: Serre wants a precise conjecture meaning that he would like to be able to read off the optimal weight and level from the Galois representation. The level has a natural intuitive definition as the Artin conductor of $\overline{\rho}$ at the primes away from p. The weight turned out to be much less intuitive –

one can suppose that this is one of the reasons why it took a long time for Serre to publish his conjecture. In the end, in part through correspondence with Fontaine, Serre figures out a precise combinatorial recipe for the weight and publishes his conjecture in 1987 [Ser87]. He writes the following to Grothendieck on the last day of 1986 (quoted from [GS04, pp. 251–252]).

> Dear Grothendieck,
>
> One of these days, you should be receiving a copy of "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$", a piece of work which I have written up over the last few months, but which has in fact been in progress for a dozen years.
>
> I would like to give you some explanation of what it is about, since you might be put off by the technical aspect of §§1, 2 and 3, and I am not sure you will really like the numerical examples in §5.
>
> You probably remember the conjecture made by Weil in 1966: every elliptic curve over $\mathbf{Q}$ is "modular". We called it the "Weil conjecture"; it is now called the "Taniyama–Weil conjecture" or the "Shimura-Taniyama conjecture", depending on the authors, but never mind. The importance of this conjecture comes from the fact that it describes how to get the simplest possible motives: those of dimension 2, height 1 and base field $\mathbf{Q}$. In particular, if the conjecture is true (and it has been checked numerically in very many cases), then the zeta function of a motive has the analytic properties (continuation and functional equation) one expects.
>
> More generally, all zeta functions attached to motives should (conjecturally) come from suitable "modular representations"; Langlands and Deligne have made fairly precise conjectures on this subject.
>
> What I tried to do in the text I am sending you is an analogue (modulo p) of this Weil conjecture. One would like to describe certain Galois representations in terms of modular forms (modulo p). These representations appear to be very special; they are representations
>
> $$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_p),$$

which are irreducible (otherwise it is not very interesting) with odd determinant (complex conjugation must have determinant -1). The conjecture I make is that all such representations are "modular", i.e. come from modular forms modulo p whose weight and level I actually predict (the recipe predicting the level is very natural – the one for the weight is not). Of course, I am not at all sure this conjecture is true! But it is supported by a large number of half-theoretical, half-numerical examples, and I have finally decided to publish it, all the more because it has many applications:

a) it implies the Weil conjecture cited above, along with analogous conjectures on motives of height > 1 (cf. §4 in my text); this may appear surprising at first: how can a result in characteristic 0 be deduced from a result in characteristic p? This is much less surprising when one realizes that there is an infinite number of p.

b) it implies Fermat's (big) theorem, along with some rather surprising variations: the non-existence of non-trivial solutions of $x^p + y^p + \ell z^p = 0$, $p \geqslant 11$, for ℓ prime equal to 3, 5, 7, 11, 17, 19, ... (but the method does not apply to $\ell = 31$).

c) it implies that any finite flat group scheme over $\mathbf{Z}$ of type (p, p) is a direct sum of copies of $\mathbf{Z}/p\mathbf{Z}$ and $\boldsymbol{\mu}_p$ (for $p \geqslant 3$). (Beware: this refers only to schemes of rank 2. I don't know how to do anything for higher rank.)

Of course, it would be slightly reassuring to be able to formulate a general conjecture (over an arbitrary global field, for representations of arbitrary dimension). I have thought about this often, but I do not see what to do (and yet I am convinced it is possible, at least in certain cases). We'll see...

Regards — and best wishes for 1987

J-P. Serre

Unfortunately for Serre, Grothendieck is not very interested. In his reply of the 25th of January 1987 he says the following (quoted from [GS04, p. 253]).

> "I realize from your letter that beautiful work is being done in math, but also and especially that such letters and the work they discuss deserve readers and commentators who are more available than I am. My research is taking me farther and farther from what is generally considered as "scientific" work (not that I have the impression of any real "break" in the ardor and the spirit I put into my work) – and anyway, it would be entirely useless for me to tell you about it, even briefly. I will talk about it, however, for those who might be interested (if any...)." – Alexander Grothendieck

Despite Grothendieck's indifference towards Serre's conjecture, it is fascinating to see the short summary Serre gives to Grothendieck. In particular, it seems that Serre was not entirely happy with his combinatorial recipe for the weight of the modular form which he deduces from the Galois representation. Although we now know that Serre's recipe for the weight was correct (in fact, Serre's entire conjecture as stated in [Ser87] is now proved), it does not seem like Serre wrote down the most intuitive way of thinking about the weight. This is something we will address in the remainder of this chapter. Another interesting fact is that Serre is already daydreaming about generalisations to more general global fields and, even, to higher dimensional representations. Later in this thesis we will extensively cover the former generalisation in the special case of *totally real fields* (i.e. extensions of $\mathbf{Q}$ such that all embeddings of the extension into $\mathbf{C}$ are contained in $\mathbf{R}$). Conjectures for other global fields or higher dimensional representations, in general, are still very much a part of ongoing research.

2.2. Cohomological reformulation of the weight

In this section we will explain how to give a cohomological reformulation of the weight appearing in Serre's conjecture. This reformulation appears for the first time in the work of Ash and Stevens [AS86b]. Since then it has been instrumental for generalisations of Serre's conjecture.

2.2.1. Serre's conjecture. Let us start with the fundamental theorem from Deligne's paper [Del71]. Let $k \geqslant 2$ and $N \geqslant 1$ be integers and suppose $f \in S_k(\Gamma_1(N), \chi)$, that is, we let f be a cuspform for $\Gamma_1(N)$ with character χ. Write the q-expansion of f as $f = \sum_{n \geqslant 1} a_n q^n$. We suppose, moreover, that f is an eigenvector for the Hecke operators which is normalised such that $a_1 = 1$. The coefficients a_n are algebraic integers. If we denote the ring of algebraic integers by $\overline{\mathbf{Z}}$, we can pick an ideal $\overline{\mathfrak{p}}$ above p. We identify the reduction $\overline{\mathbf{Z}}/\overline{\mathfrak{p}}$ with $\overline{\mathbf{F}}_p$ and we may therefore consider reductions of algebraic integers to lie in $\overline{\mathbf{F}}_p$. Then by the process described in the previous section, we immediately get the following theorem.

THEOREM 2.2.1 (Deligne). *Suppose $k \geqslant 2$ and $N \geqslant 1$. Let f be a modular form in $S_k(\Gamma_1(N), \chi)$, which is an eigenform for the Hecke operators. Then there exists a unique semisimple mod p Galois representation*

$$\overline{\rho}_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p),$$

such that for all $\ell \nmid Np$

- *$\overline{\rho}$ is unramified at ℓ;*
- $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_\ell) = \overline{a_\ell}$;
- *and* $\det \overline{\rho}(\mathrm{Frob}_\ell) = \overline{\chi(\ell)\ell^{k-1}}$.

Suppose that we are given a representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ which is irreducible and odd, meaning that for $c \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ the automorphism of $\overline{\mathbf{Q}}$ given by complex conjugation we have $\det \overline{\rho}(c) = -1$. In [Ser87] there is a precise recipe for constructing integers $N(\overline{\rho}) \geqslant 1$ and $k(\overline{\rho}) \geqslant 2$ and a character $\chi(\overline{\rho})$ depending on the representation only. In fact, the recipe for the integer $k(\overline{\rho})$ only depends on the restriction $\overline{\rho}|_{I_{\mathbf{Q}_p}}$. The integer $N(\overline{\rho})$ is defined as the Artin conductor away from p and will therefore by construction always be prime to p. For the details of the construction of $k(\overline{\rho})$ and $\chi(\overline{\rho})$ we refer the reader to [Ser87]. Serre's conjecture on modular forms can then be phrased as follows.

CONJECTURE 2.2.2. *Given $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$, which is odd and irreducible, there exists a cusp form f of weight $k(\overline{\rho})$, level $\Gamma_1(N(\overline{\rho}))$ and character $\chi(\overline{\rho})$, which is an eigenvector for the Hecke operators, such that $\overline{\rho} \cong \overline{\rho}_f$.*

It should be noted that this conjecture is a theorem now due to the work of many authors culminating in the work of Khare and Wintenberger in [KW09a] and [KW09b]. An important ingredient in their proof is Edixhoven's proof in [Edi92] that Serre's recipe for the weight does, in fact, correctly predict the minimal possible weight of a modular form associated to $\overline{\rho}$. This is what is sometimes referred to as the weight part of Serre's conjecture.

2.2.2. A cohomological reformulation. We will now explain how to reformulate the weight $k(\overline{\rho})$ in Serre's conjecture above in terms of Galois cohomology. This point of view appears first in the work of Ash and Stevens [AS86b].

Suppose $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is odd and irreducible as above. Let us also fix N to be the Artin conductor of $\overline{\rho}$ away from p. In particular, N is coprime to p. For any $k \geqslant 2$, we denote the $(k-2)$th symmetric power of the standard representation of $\mathrm{GL}_2(\mathbf{F}_p)$ on $\overline{\mathbf{F}}_p^2$ by $\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$. Hence, $\Gamma_1(N) \subseteq \mathrm{SL}_2(\mathbf{Z})$ also acts on $\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$ via its reduction to a subgroup of $\mathrm{SL}_2(\mathbf{F}_p)$. Recall that we have the Hecke algebra of $\Gamma_1(N)$, defined in terms of double coset operators, acting on the group cohomology groups $H^1(\Gamma_1(N), \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)$. We will say that $\overline{\rho}$ **occurs** in $H^1(\Gamma_1(N), \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)$ if we can find an eigenvector for the Hecke operators in this vector space with eigenvalues $\mathrm{Tr}\,\overline{\rho}(\mathrm{Frob}_\ell)$ for all $\ell \nmid pN$. We can then use the Eichler–Shimura isomorphism to prove that $\overline{\rho}$ is modular of weight k and level N (in the sense of Conjecture 2.2.2) if and only if $\overline{\rho}$ occurs in $H^1(\Gamma_1(N), \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)$. Since we do not know of a good reference for this classical result, let us give a proof here.

2.2.2.1. *Modularity and* $H^1(\Gamma, \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)$. Given an irreducible continuous Galois representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ which is unramified at ℓ for all $\ell \nmid pN$, we define certain maximal ideals in rings of Hecke operators. We let $\tilde{\mathbb{T}}_{\mathbf{Z}}$ be the abstract $\mathbf{Z}$-algebra of Hecke operators $\mathbf{Z}[\ldots, T_\ell, \ldots]$ for $\ell \nmid pN$. Then we have a homomorphism $\tilde{\mathbb{T}}_{\mathbf{Z}} \to \overline{\mathbf{F}}_p$ defined by sending $T_\ell \to \mathrm{Tr}\,\rho(\mathrm{Frob}_\ell)$. Denote the kernel of this homomorphisms by $\mathfrak{m}_\rho$. Similarly, we get an ideal $\overline{\mathfrak{m}}_\rho$ of $\tilde{\mathbb{T}}_{\overline{\mathbf{F}}_p} := \tilde{\mathbb{T}}_{\mathbf{Z}} \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p$ defined again as the kernel of the map evaluating the Hecke operators at the traces of Frobenius. Since the image of these homomorphisms are finite subrings of an integral domain, hence a field, the ideals $\mathfrak{m}_\rho$ and $\overline{\mathfrak{m}}_\rho$ will be maximal. We will say that a maximal ideal in a Hecke-module is **Eisenstein** if the associated Galois representation is reducible. A Hecke-module is Eisenstein if all the maximal ideals in its support are Eisenstein. For simplicity we will assume $N > 4$ so that $\Gamma_1(N)$ is sufficiently small (see [DI95, §12.1]) and sometimes we will denote this group simply by Γ.

DEFINITION 2.2.3. We will say that ρ is **cohomologically modular** of weight $k \geqslant 2$ and level N if

$$H^1(\Gamma_1(N), \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)_{\overline{\mathfrak{m}}_\rho} \neq 0.$$

We begin with the following lemma which shows that it does not matter whether our rings are defined over $\overline{\mathbf{F}}_p$ or $\mathbf{F}_p$. The proof of the lemma is just standard commutative algebra.

LEMMA 2.2.4. *For $k \geqslant 2$ and $\Gamma := \Gamma_1(N)$, we have that*

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)_{\overline{\mathfrak{m}}_\rho} \neq 0$$

if and only if

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)_{\mathfrak{m}_\rho} \neq 0.$$

PROOF. Since $(p) \subset \mathrm{Ann}_{\tilde{\mathbb{T}}_{\mathbf{Z}}}\left(H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)\right)$, without loss of generality we may consider it to be an $\tilde{\mathbb{T}}_{\mathbf{F}_p} := \tilde{\mathbb{T}}_{\mathbf{Z}} \otimes \mathbf{F}_p$-module and replace $\mathfrak{m}_\rho$ by the maximal ideal $\mathfrak{m}'_\rho$ in $\tilde{\mathbb{T}}_{\mathbf{F}_p}$ also defined by evaluating Hecke operators at traces of Frobenius.

By the universal coefficient theorem, we have that

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2) \cong H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2) \otimes \overline{\mathbf{F}}_p.$$

We recall that localisation at a prime ideal is non-zero if and only if the prime ideal contains the annihilator of the module. Letting R denote the Hecke ring $\tilde{\mathbb{T}}_{\mathbf{F}_p}$ and letting M denote $H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)$ as an R-module, we have to prove that $\mathfrak{m}'_\rho \supset \mathrm{Ann}_R(M)$ if and only if $\overline{\mathfrak{m}}_\rho \supset \mathrm{Ann}_{R\otimes\overline{\mathbf{F}}_p}(M \otimes \overline{\mathbf{F}}_p)$.

By tensoring the exact sequence defining the former annihilator by $\overline{\mathbf{F}}_p$ we get

$$0 \to \mathrm{Ann}_R(M) \otimes \overline{\mathbf{F}}_p \to R \otimes \overline{\mathbf{F}}_p \to \mathrm{End}_{\mathbf{F}_p}(M) \otimes \overline{\mathbf{F}}_p.$$

Since M is finite dimensional, $\mathrm{End}_{\mathbf{F}_p}(M) \otimes \overline{\mathbf{F}}_p \cong \mathrm{End}_{\overline{\mathbf{F}}_p}(M \otimes \overline{\mathbf{F}}_p)$. It follows that $\mathrm{Ann}_R(M) \otimes \overline{\mathbf{F}}_p \cong \mathrm{Ann}_{R\otimes\overline{\mathbf{F}}_p}(M \otimes \overline{\mathbf{F}}_p)$.

Under the canonical inclusion $\tilde{\mathbb{T}}_{\mathbf{F}_p} \hookrightarrow \tilde{\mathbb{T}}_{\overline{\mathbf{F}}_p}$ we have that $\mathfrak{m}'_\rho \subset \overline{\mathfrak{m}}_\rho$. Suppose that $\mathfrak{m}'_\rho \supset \mathrm{Ann}_R(M)$. Then

$$\mathfrak{m}'_\rho \otimes \overline{\mathbf{F}}_p \supset \mathrm{Ann}_R(M) \otimes \overline{\mathbf{F}}_p = \mathrm{Ann}_{R\otimes\overline{\mathbf{F}}_p}(M \otimes \overline{\mathbf{F}}_p).$$

But $\overline{\mathfrak{m}}_\rho \supset \mathfrak{m}'_\rho \otimes \overline{\mathbf{F}}_p$ as $\overline{\mathfrak{m}}_\rho \supset \mathfrak{m}'_\rho$, so $\overline{\mathfrak{m}}_\rho \supset \mathrm{Ann}_{R\otimes\overline{\mathbf{F}}_p}(M \otimes \overline{\mathbf{F}}_p)$.

On the other hand, suppose that $\overline{\mathfrak{m}}_\rho \supset \mathrm{Ann}_{R\otimes\overline{\mathbf{F}}_p}(M \otimes \overline{\mathbf{F}}_p)$. We note that the intersection $\overline{\mathfrak{m}}_\rho \cap R$ is a maximal ideal of R containing $\mathfrak{m}'_\rho$, hence equal to $\mathfrak{m}'_\rho$. Therefore, $\mathfrak{m}'_\rho \supset \mathrm{Ann}_{R\otimes\overline{\mathbf{F}}_p}(M \otimes \overline{\mathbf{F}}_p) \cap R$. The latter is, by definition, equal to $\mathrm{Ann}_R(M \otimes \overline{\mathbf{F}}_p)$, which simply equals $\mathrm{Ann}_R(M)$. $\square$

Next we prove that we may even lift our rings (defined over $\mathbf{F}_p$) to characteristic 0. The proof of this lemma is not just simply commutative algebra anymore, but we use that ρ is irreducible and that Γ is a free group.

LEMMA 2.2.5. *For $k \geqslant 2$ and $\Gamma := \Gamma_1(N)$, we have that*

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)_{\mathfrak{m}_\rho} \neq 0$$

if and only if

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \neq 0.$$

PROOF. We have a short exact sequence

$$0 \to \mathrm{Sym}^{k-2}\mathbf{Z}^2 \xrightarrow{\cdot p} \mathrm{Sym}^{k-2}\mathbf{Z}^2 \to \mathrm{Sym}^{k-2}\mathbf{F}_p^2 \to 0.$$

Since p is the only prime in the ideal $\mathfrak{m}_\rho$, the space $H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho}$ has no ℓ-torsion for any $\ell \neq p$. Moreover, by the exactness of localisation, we get a long exact sequence

$$H^0(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)_{\mathfrak{m}_\rho} \to H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \xrightarrow{\cdot p} H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho}.$$

Since the Hecke action on $H^0(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)$ is Eisenstein and ρ is irreducible, localising at $\mathfrak{m}_\rho$ gives 0. Hence, we conclude that $H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho}$ has no p-torsion either. In other words this space is torsion-free.

On the other hand we get the long exact sequence

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \xrightarrow{\cdot p} H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \to H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)_{\mathfrak{m}_\rho} \to 0,$$

where the last term is zero since Γ is a free group. Since $H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho}$ is torsion-free, we get that $H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \neq 0$ if and only if

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \otimes \mathbf{F}_p \neq 0,$$

which, by the long exact sequence, happens if and only if $H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{F}_p^2)_{\mathfrak{m}_\rho}$ does not vanish. □

We define the parabolic cohomology $H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)$ as the intersection of the kernels of the restriction maps

$$\mathrm{res}_\alpha : H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2) \to H^1(\Gamma_\alpha, \mathrm{Sym}^{k-2}\mathbf{R}^2)$$

where $\alpha \in \mathbf{P}(\mathbf{Q})$ runs over all cusps and Γ_α denotes the stabiliser of α. Then the Eichler–Shimura isomorphism (see, for example, [RS01, p. 169]) gives a Hecke equivariant isomorphism of $\mathbf{R}$-vector spaces

$$S_k(\Gamma, \mathbf{C}) \xrightarrow{\cong} H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2).$$

Therefore, we are interested in extending from $\mathbf{Z}$-coefficients to $\mathbf{R}$-coefficients and taking parabolic cohomology to put ourselves in the context of the Eichler–Shimura isomorphism. We will do this in the following lemma.

LEMMA 2.2.6. *For $k \geqslant 2$ and $\Gamma := \Gamma_1(N)$, we have that*

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \neq 0$$

if and only if

$$H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \neq 0.$$

PROOF. By the universal coefficient theorem, as $\mathbf{R}$ is $\mathbf{Z}$-flat, we have that

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \otimes_{\mathbf{Z}} \mathbf{R} \cong H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho}.$$

Hence, since $H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho}$ is torsion-free, we get

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{Z}^2)_{\mathfrak{m}_\rho} \neq 0$$

if and only if

$$H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \neq 0.$$

To relate this to parabolic cohomology we consider the short exact sequence

$$0 \to H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \to H^1(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \to E_{\mathfrak{m}_\rho} \to 0,$$

where E is simply defined as the quotient making the sequence

$$H^1_p \to H^1 \to E \to 0$$

exact. It follows from the various Eichler–Shimura isomorphisms that the Hecke action on the quotient E is Eisenstein. Since ρ was assumed to be irreducible, we get that $E_{\mathfrak{m}_\rho} = 0$. □

Now we are finally in the position that we can relate the non-vanishing of the localisation of this cohomology group to the existence of an eigenform with an isomorphic mod p Galois representation. In other words, in the following lemma (combined with the previous lemmas) we will prove that ρ is cohomologically modular of weight k and level N if and only if ρ is modular of weight k and level N in the usual sense.

LEMMA 2.2.7. *For $k \geqslant 2$ and $\Gamma := \Gamma(N)$, we get that*

$$H^1_p(\Gamma_1(N), \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \neq 0$$

if and only if

$$\rho \cong \overline{\rho}_f$$

for some eigenform f of weight k and level N.

Proof. We let $\mathbb{T}_{\mathbf{Z}}$ denote the image of $\tilde{\mathbb{T}}_{\mathbf{Z}}$ in $\mathrm{End}(H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2))$, so $\mathbb{T}_{\mathbf{Z}}$ is now a finitely generated free $\mathbf{Z}$-module.

Suppose first that $\rho \cong \overline{\rho}_f$ for some eigenform f of weight k and level N. Then we get the following homomorphisms:

(1) $\mathbb{T}_{\mathbf{Z}} \to \mathcal{O}_f$ defined by $T_\ell \mapsto a_\ell(f)$, where $\mathcal{O}_f$ is the ring of integers of the number field defined by the coefficients of the Fourier expansion of f. Call the kernel of this homomorphism $\mathfrak{p}_f$.

(2) $\mathbb{T}_{\mathbf{Z}} \to \mathcal{O}_f \to \overline{\mathbf{F}}_p$, which is the composition of the first homomorphism with the reduction at a prime ideal above p such that $\overline{a}_\ell(f) = \mathrm{Tr}\,\rho(\mathrm{Frob}_\ell)$ for all $\ell \nmid pN$. The kernel of this homomorphism is $\mathfrak{m}_\rho$ (or, rather, it's image in $\mathbb{T}_{\mathbf{Z}}$).

We recall that for a general ring R, an R-module M and a prime ideal $\mathfrak{p}$ of R, we have that $M_{\mathfrak{p}} \neq 0$ if and only if $\mathfrak{p}$ contains $\mathrm{Ann}_R(M)$. But, by definition, $\mathfrak{m}_\rho$ contains $\mathfrak{p}_f$. Moreover, if $T \in \mathrm{Ann}(H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2))$, then $Tf = 0$ and so $T \in \mathfrak{p}_f$. Hence, $\mathfrak{p}_f$ must contain $\mathrm{Ann}(H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2))$. We conclude that $H^1_p(\Gamma_1(N), \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \neq 0$.

Now suppose that $H^1_p(\Gamma_1(N), \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \neq 0$. Since $\mathbb{T}_{\mathbf{Z}}$ is a finite free $\mathbf{Z}$-module, the going down theorem tells us that there exists a minimal prime $\mathfrak{p} \subseteq \mathfrak{m}_\rho$ such that $\mathfrak{p} \cap \mathbf{Z} = (0)$. Then $\mathfrak{p}_{\mathbf{Q}} := \mathfrak{p} \otimes \mathbf{Q}$ defines a prime ideal in $\mathbb{T}_{\mathbf{Q}} := \mathbb{T} \otimes \mathbf{Q}$. The ring $\mathbb{T}_{\mathbf{Q}}$ is Artinian and therefore we get that $H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{p}_{\mathbf{Q}}} \neq 0$ if and only if $H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)[\mathfrak{p}_{\mathbf{Q}}] \neq 0$, where the latter group denotes the kernel of multiplication by $\mathfrak{p}_{\mathbf{Q}}$. Moreover, we know that $H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{p}_{\mathbf{Q}}} \neq 0$ since $H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)_{\mathfrak{m}_\rho} \neq 0$ and $\mathfrak{m}_\rho$ contains $\mathfrak{p}$.

However, $H^1_p(\Gamma, \mathrm{Sym}^{k-2}\mathbf{R}^2)[\mathfrak{p}_{\mathbf{Q}}] \neq 0$ means by the Eichler–Shmiura isomorphism that there is an eigenform f with eigenvalues defined as the images

$$\begin{aligned} \mathbb{T}_{\mathbf{Q}} &\to \mathbb{T}_{\mathbf{Q}}/\mathfrak{p}_{\mathbf{Q}}, \\ T_\ell &\mapsto a_\ell. \end{aligned}$$

It is now clear that for this form we have that $\rho \cong \overline{\rho}_f$. □

2.2.2.2. *Serre weights.* It turns out that, instead of considering the representations $\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$, it is possible to pass to Jordan–Hölder factors, which will lead us naturally to the definition of a Serre weight. Let us describe how to do this now. Suppose that ρ is cohomologically modular of weight $k \geqslant 2$ and level $N > 4$, where N is the Artin conductor away from p.

Since $\Gamma := \Gamma_1(N)$ is sufficiently small, the quotient map $\mathcal{H} \to \mathcal{H}/\Gamma$ gives a universal cover allowing us to relate group cohomology of Γ to the cohomology of the modular curve $Y := \mathcal{H}/\Gamma$. For example, it is explained in [DI95, p. 108] that for any subquotient A of $\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$ we can identify $H^2(\Gamma, A)$ with $H^2(Y, \underline{A})$ for a locally constant sheaf of sections $\underline{A}$ constructed from A. Then its follows from Poincaré duality that $H^2(Y, \underline{A}) \cong H^0_{\mathrm{c}}(Y, \underline{A})$, which vanishes by the non-compactness of the modular curve Y. So $H^2(\Gamma, A) = 0$ for any subquotient A of $\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$.

On the other hand, since ρ is irreducible and the Hecke action on $H^0(\Gamma, A)$ is Eisenstein, it follows that $H^0(\Gamma, A)_{\overline{\mathfrak{m}}_\rho} = 0$. Therefore, by exactness of localisation, for any short exact sequence $0 \to A \to B \to C \to 0$ we get a short exact sequence

$$0 \to H^1(\Gamma, A)_{\overline{\mathfrak{m}}_\rho} \to H^1(\Gamma, B)_{\overline{\mathfrak{m}}_\rho} \to H^1(\Gamma, C)_{\overline{\mathfrak{m}}_\rho} \to 0.$$

If $0 = W_0 \subset W_1 \subset \cdots \subset W_n = \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$ is a Jordan–Hölder composition series with each $V_{i+1} := W_{i+1}/W_i$ irreducible, then from the short exact sequence it follows that $H^1(\Gamma_1(N), \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)_{\overline{\mathfrak{m}}_\rho} \neq 0$ if and only if $H^1(\Gamma, V_j)_{\overline{\mathfrak{m}}_\rho} \neq 0$ for some $1 \leqslant j \leqslant n$.

We have just shown that $\overline{\rho}$ occurs in $H^1(\Gamma_1(N), \mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2)$ if and only if it occurs in $H^1(\Gamma_1(N), V)$ for some Jordan–Hölder factor V of $\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$ as a $\mathrm{GL}_2(\mathbf{F}_p)$-representation (alternatively, this is proved in [AS86a, Lem. 2.1]). This suggests the following definition.

Definition 2.2.8. A **Serre weight** is an irreducible $\overline{\mathbf{F}}_p$-representation of $\mathrm{GL}_2(\mathbf{F}_p)$. These can all be given uniquely in the form (see, for example, [BL94, Prop. 1])

$$V_{a,b} := \det{}^b \otimes_{\mathbf{F}_p} \mathrm{Sym}^{a-b}\overline{\mathbf{F}}_p^2$$

where $0 \leqslant a - b \leqslant p - 1$ and $0 \leqslant b < p - 1$.

We give the following reformulation of the weights associated to $\overline{\rho}$.

Definition 2.2.9. The set of Serre weights $W(\overline{\rho})$ associated to $\overline{\rho}$ is defined by

$$W(\overline{\rho}) := \left\{\text{Serre weights } V \mid \overline{\rho} \text{ occurs in } H^1(\Gamma_1(N), V)\right\}.$$

We note that we chose N to be the Artin conductor of $\overline{\rho}$ away from N, but by the correctness of Serre's recipe we could have equivalently given the definition of $W(\overline{\rho})$ as the set of all Serre weights V such that $\overline{\rho}$ occurs in $H^1(\Gamma_1(N'), V)$ for some N' which is coprime to p.

2.3. Serre weights and crystalline lifts

In this section we would like to phrase our cohomological definition in terms of p-adic Hodge theory. For a brief overview of the theory and conventions used, we refer the reader to §1.2.

2.3.1. Crystalline lifts. We already saw that for $2 \leqslant k \leqslant p+1$ we have that $\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2$ is irreducible. Therefore, by Section 2.2.2, we have that

$$\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2 \in W(\overline{\rho}) \iff \overline{\rho} \text{ is modular of weight } k \text{ and level } (N,p)=1.$$

This means, by definition, that there exists a modular form f of weight k and level N (coprime to p) such that $\overline{\rho} \cong \overline{\rho}_f$. Then the representation $\rho_f|_{G_{\mathbf{Q}_p}}$ gives a characteristic zero lift of $\overline{\rho}|_{G_{\mathbf{Q}_p}}$. By [Fal87] and [FJ95] the representation $\rho_f|_{G_{\mathbf{Q}_p}}$ is crystalline (since N is coprime to p) and has Hodge–Tate weights $\{k-1,0\}$. We get the implication

$$\mathrm{Sym}^{k-2}\overline{\mathbf{F}}_p^2 \in W(\overline{\rho}) \implies \overline{\rho}|_{G_{\mathbf{Q}_p}} \text{ has a crystalline lift to characteristic zero}$$
$$\text{with Hodge–Tate weights } \{k-1,0\}.$$

Twists by det on the Serre weight side correspond to twists by the mod p cyclotomic character on the representation side – we will see this again later. This means that $W(\overline{\varepsilon}^b \otimes \overline{\rho}) = \{\det{}^b \otimes V \mid V \in W(\overline{\rho})\}$. Therefore, including twists in the above, we get the implication

$$V_{a,b} \in W(\overline{\rho}) \implies \overline{\rho}|_{G_{\mathbf{Q}_p}} \text{ has a crystalline lift to characteristic zero}$$
$$\text{with Hodge–Tate weights } \{a+1,b\}.$$

The key idea in the area of the Serre weight conjectures is that this implication is an if and only if! Vaguely speaking the philosophy is as follows: the existence of a local crystalline lift of the prescribed Hodge–Tate weights should be explained by the fact that there exists a global lift to a representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ which is unramified almost everywhere and whose restriction to $G_{\mathbf{Q}_p}$ gives such a local lift. Then by the Fontaine–Mazur and Langlands conjectures such representations come from modular forms of the required weight and a level coprime to p.

In the case above (that is, the case of GL_2 over $\mathbf{Q}$) enough is known about the various conjectures above that we can indeed verify that the implication is an if and only if, but in greater generality we can use this observation as a guiding principle which allows us to give a definition of $W(\overline{\rho})$ which generalises more easily. The new definition will be as follows.

DEFINITION 2.3.1. The set of Serre weights $W(\overline{\rho})$ associated to $\overline{\rho}$ is defined to be the set

$$\left\{ \text{Serre weights } V_{a,b} \,\middle|\, \overline{\rho}|_{G_{\mathbf{Q}_p}} \text{ has a crystalline lift of HT-weights } \{a+1, b\} \right\}.$$

2.3.2. A companion forms example. To give an example of this principle we consider the case where

$$\overline{\rho}|_{G_{\mathbf{Q}_p}} \cong \begin{pmatrix} \lambda\overline{\varepsilon}^a & * \\ 0 & \mu\overline{\varepsilon}^b \end{pmatrix}$$

for $1 < a - b < p - 2$, $b \geqslant 0$ and unramified characters λ and μ. If the extension class $*$ is non-split, it turns out there is only one possibility for the Hodge–Tate weights of crystalline lifts and we get that

$$W(\overline{\rho}) = \{V_{a-1,b}\} = \{\det{}^b \otimes \mathrm{Sym}^{a-b-1}\overline{\mathbf{F}}_p^2\}.$$

On the other hand, if the extension class vanishes we can write down multiple possibilities for the Hodge–Tate weights of crystalline lifts. Namely, one lift is given by

$$\begin{pmatrix} \tilde{\lambda}\varepsilon^a & 0 \\ 0 & \tilde{\mu}\varepsilon^b \end{pmatrix}$$

where $\tilde{\lambda}, \tilde{\mu}$ are Teichmüller lifts of the unramified characters. This representation has Hodge–Tate weights $\{a, b\}$. Another lift is given by

$$\begin{pmatrix} \tilde{\lambda}\varepsilon^a & 0 \\ 0 & \tilde{\mu}\varepsilon^{b+p-1} \end{pmatrix},$$

which has Hodge–Tate weights $\{b + p - 1, a\}$. We get two Serre weights associated to $\overline{\rho}$, i.e. $W(\overline{\rho})$ is equal to

$$\{V_{a-1,b}, V_{b+p-2,a}\} = \{\det{}^b \otimes \mathrm{Sym}^{a-b-1}\overline{\mathbf{F}}_p^2, \det{}^a \otimes \mathrm{Sym}^{b-a+p-2}\overline{\mathbf{F}}_p^2\}.$$

This example is closely related to an observation made by Serre called the "companion forms" phenomenon. When $\overline{\rho}$ satisfies

$$\overline{\rho}|_{I_{\mathbf{Q}_p}} \cong \begin{pmatrix} \overline{\varepsilon}^{k-1} & * \\ 0 & 1 \end{pmatrix}$$

and $2 < k < p + 1$, Serre's recipe for the weight says that $k(\overline{\rho}) = k$. Given a reducible representation $\overline{\rho} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ we can always take a twist by a power of $\overline{\varepsilon}$ to make sure $\overline{\rho}|_{I_{\mathbf{Q}_p}}$ is an extension of 1 by a power of $\overline{\varepsilon}$ and we can always take the power to lie in $[1, p]$. However, if for $\overline{\rho}|_{I_{\mathbf{Q}_p}}$ as above also $*$ vanishes and $k < p-1$ then we have that

$$(\overline{\rho} \otimes \overline{\varepsilon}^{1-k})\big|_{I_{\mathbf{Q}_p}} \cong \begin{pmatrix} \overline{\varepsilon}^{p-k} & 0 \\ 0 & 1 \end{pmatrix}.$$

So there are, in fact, two twists of the right form. These correspond to two "companion forms" associated to $\overline{\rho}$ and its twist.

CHAPTER 3

Serre weights for totally real fields

In this chapter we explain how to extend the ideas of the previous chapter to modular forms over totally real number fields (i.e. Hilbert modular forms). We will start with a very brief overview of the theory of Hilbert modular forms. Then we turn to the paper of Buzzard, Diamond and Jarvis [BDJ10] to see how we can define modularity via Serre weights in this context. We will end with a careful statement of the modularity conjecture in the locally reducible case.

In this chapter we introduce the relevant theory which will be studied later in this thesis. None of the work presented here is original to the author. The relevant sources are cited at the beginning of the sections and throughout the text.

3.1. Hilbert modular forms

In this section we will give a brief overview of the theory of Hilbert modular forms. This global automorphic theory clearly underlies the study of Serre weights and, therefore, it is an important motivation for the main results of this thesis. However, since the main results of this thesis will all be of a local nature, we will only give brief sketches of the global theory. More extensive treatments of the theory of Hilbert modular forms can be found in Garrett [Gar89] or in Freitag [Fre90]. Also, the article of Dembélé and Voight [DV13] gives a nice brief overview of the theory.

Let F be a totally real field of degree $[F : \mathbf{Q}] = d > 1$, i.e. a finite extension of $\mathbf{Q}$ such that the image of every embedding $\tau\colon F \hookrightarrow \mathbf{C}$ is contained in $\mathbf{R}$, and let $\Sigma_F := \{\sigma_1, \ldots, \sigma_d\colon F \hookrightarrow \mathbf{R}\}$ denote the set of all embeddings. For simplicity we will assume F has strict class number 1. Let $G := \mathrm{Res}_{F/\mathbf{Q}}\mathrm{GL}_2$ be the algebraic group obtained by restricting scalars from F to $\mathbf{Q}$; or, equivalently, define $G(R) := \mathrm{GL}_2(R \otimes_{\mathbf{Q}} F)$ for any $\mathbf{Q}$-algebra R. Then we have $G(\mathbf{R}) := \mathrm{GL}_2(\mathbf{R} \otimes_{\mathbf{Q}} F) = \prod_{\sigma\in\Sigma_F} \mathrm{GL}_2(\mathbf{R})$. We define

$$G(\mathbf{R})^+ := \{g = (g_\sigma)_{\sigma\in\Sigma_F} \mid \det(g_\sigma) > 0 \text{ for all } \sigma \in \Sigma_F\}.$$

Note that $G(\mathbf{Q}) = \mathrm{GL}_2(F)$. This group naturally embeds into $G(\mathbf{R})$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \sigma(a) & \sigma(b) \\ \sigma(c) & \sigma(d) \end{pmatrix}_{\sigma\in\Sigma_F}$$

and we identify $G(\mathbf{Q})$ with its image. We set $G(\mathbf{Q})^+ := G(\mathbf{Q}) \cap G(\mathbf{R})^+$.

Definition 3.1.1. Let Γ be a subgroup of $G(\mathbf{Q})^+$. We say that Γ is a **congruence subgroup** if there exists a compact open subgroup $K \subseteq G(\mathbb{A}_F^\infty)$ such that

$$\Gamma = G(\mathbf{Q}) \cap KG(\mathbb{A}_{F,\infty})^+,$$

where $\mathbb{A}_F^\infty$ and $\mathbb{A}_{F,\infty}$ denote the finite and infinite adèles of F, respectively.

If $\mathfrak{N} \subseteq \mathcal{O}_F$ is a non-zero ideal, then we let

$$\Gamma_0(\mathfrak{N}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_F)^+ \mid c \in \mathfrak{N} \right\}.$$

We need to define an action of these groups on d copies of the complex upper half plane. We let $\mathcal{H} := \{z \in \mathbf{C} \mid \mathrm{Im}(z) > 0\}$ denote the upper half of the complex plane. We take d copies of the upper half plane by defining

$$\mathcal{H}_F := \{(z_\sigma)_{\sigma\in\Sigma_F} \mid z_\sigma \in \mathcal{H} \text{ for all } \sigma \in \Sigma_F\}.$$

Then $G(\mathbf{R})^+$ acts on $\mathcal{H}_F$ as follows: for any $\gamma = (\gamma_\sigma)_{\sigma\in\Sigma_F} \in G(\mathbf{R})^+$ and $z = (z_\sigma)_{\sigma\in\Sigma_F} \in \mathcal{H}_F$ we define $\gamma \cdot z := (\gamma_\sigma \cdot z_\sigma)_{\sigma\in\Sigma_F}$ via

$$\gamma_\sigma \cdot z_\sigma := \frac{a_\sigma z_\sigma + b_\sigma}{c_\sigma z_\sigma + d_\sigma}, \text{ where } \gamma_\sigma = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}.$$

We let $\underline{k} = (k_\sigma)_\sigma \in (\mathbf{Z}_{\geqslant 1})^{\Sigma_F}$ be a tuple of integers such that

$$k_{\sigma_1} \equiv k_{\sigma_2} \equiv \cdots \equiv k_{\sigma_d} \bmod 2.$$

We let $k' := \max\{k_\sigma \mid \sigma \in \Sigma_F\}$, and define $\underline{m}, \underline{t} \in \mathbf{Z}^{\Sigma_F}$ by $m_\sigma = \frac{k'-k_\sigma}{2}$ and $\underline{t} = (1, 1, \ldots, 1)$. For $z = (z_\sigma)_\sigma \in \mathcal{H}$ and $\gamma = (\gamma_\sigma)_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G(\mathbf{R})^+$ we let

$$j(\gamma, z)^{-\underline{k}} := \prod_{\sigma\in\Sigma_F} (c_\sigma z_\sigma + d_\sigma)^{-k_\sigma}.$$

For any function $f\colon \mathcal{H}_F \to \mathbf{C}$ and $\gamma \in \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G(\mathbf{Q})^+$ we may then define $f|_{\underline{k}}\gamma\colon \mathcal{H}_F \to \mathbf{C}$ by

$$(f|_{\underline{k}}\gamma)(z) = \det(\gamma)^{\underline{k}+\underline{m}-\underline{t}} j(\gamma, z)^{-\underline{k}} f(\gamma z).$$

This defines a group action: one checks easily that $f|_{\underline{k}}\gamma_1\gamma_2 = (f|_{\underline{k}}\gamma_1)|_{\underline{k}}\gamma_2$.

Definition 3.1.2. Let Γ be a congruence subgroup and $\underline{k}$ as above. A (classical) **Hilbert modular form** of level Γ and weight $\underline{k}$ is a holomorphic function $f\colon \mathcal{H}_F \to \mathbf{C}$ such that $f|_{\underline{k}}\gamma = f$ for all $\gamma \in \Gamma$. If $\Gamma = \Gamma_0(\mathfrak{N})$ for a non-zero ideal $\mathfrak{N} \subseteq \mathcal{O}_F$, then we also say f is of level $\mathfrak{N}$.

We have decided to stick to $\Gamma_0(\mathfrak{N})$ for the sake of simplicity. We note, however, that it is not too complicated to extend this definition to $\Gamma_1(\mathfrak{N})$ (defined by additionally requiring $d \equiv 1 \bmod \mathfrak{N}$ for matrices in $\Gamma_0(\mathfrak{N})$). Similarly to the case of classical modular forms, we would then have a character appearing in the definition above and in the determinant condition of Theorem 3.1.3 below (which will now be a ray class character of conductor dividing $\mathfrak{N}$).

Omitting the details for sake of brevity (see, for example, [DV13]) we will now state that these Hilbert modular forms have q-expansions and they are called cuspforms if the 0th coefficient vanishes. Analogously to the $F = \mathbf{Q}$ case, it is possible to give a coherent theory of Hecke operators $T_{\mathfrak{n}}$ indexed by non-zero ideals $\mathfrak{n} \subseteq \mathcal{O}_F$ acting on the spaces of Hilbert modular forms of a fixed weight and level. Then the following is a theorem of Carayol, Taylor, Blasius–Rogawski and Jarvis (see [Jar97]).

Theorem 3.1.3. *Let f be a Hilbert modular cuspform of weight $\underline{k}$ and level $\mathfrak{N}$ which is an eigenform for the Hecke operators with $T_{\mathfrak{n}}$ having eigenvalue $a_{\mathfrak{n}}$. Furthermore, let K denote the number field generated by the eigenvalues and let λ be a prime of $\mathcal{O}_K$ lying above the integral prime $\ell \in \mathbf{Z}$.*

Then there exists a continuous representation

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\mathcal{O}_{K,\lambda}),$$

which is unramified outside $\mathfrak{N}\ell$, and such that for any prime $\mathfrak{p}$ of $\mathcal{O}_F$ not diving $\mathfrak{N}\ell$ we have that

$$\mathrm{Tr}\,\rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}}) = a_{\mathfrak{p}};$$
$$\det \rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}}) = N_{F/\mathbf{Q}}(\mathfrak{p})^{k'-1}.$$

We remark that in all of the above we restrict ourselves to the case of totally real fields because we have no good way of constructing Galois representations for general number fields (although now it is possible to construct Galois representations for CM fields). The main issue is the lack of nice algebraic varieties over general number fields in whose cohomology we could look for our Galois representations. Over totally real fields we have the theory of Shimura varieties which has no good analogue over general number fields.

3.2. The weight recipe for totally real fields

In this section we will describe briefly what goes into giving a precise recipe for the set of weights attached to a mod p Galois representation of the absolute Galois group of a totally real field F. This recipe should be analogous to Serre's recipe of the weight for the case $F = \mathbf{Q}$. The first time a precise recipe was given was in the paper of Buzzard, Diamond and Jarvis [BDJ10]. Their construction depends completely on a cohomological reformulation of the weight analogous to the reformulation sketched in the previous chapter. The set of weights is then given in terms of crystalline lifts analogous to what we presented in Section 2.3 of the previous chapter for the case $F = \mathbf{Q}$.

The relation between the (classical) weight of a Hilbert modular form and the Serre weights of Buzzard, Diamond and Jarvis is described in detail in [BDJ10, §2]. Setting-up the machinery properly is somewhat technical and, as these sections only serve as motivation for our later results, we have chosen not to give all details but rather give a brief sketch of the most important results. For more details we refer the reader to [BDJ10, §2].

3.2.1. Modularity via Serre weights. Given a Hilbert modular cuspform f, which is an eigenform for the Hecke operators, Theorem 3.1.3 associates to f a Galois representation ρ_f. By taking a lattice fixed by this representation, reducing modulo p and taking the semisimplification, we obtain a well-defined mod p representation

$$\overline{\rho}_f : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$$

associated to f. One then expects the following "folklore" generalisation of Serre's conjecture to hold.

Conjecture 3.2.1. *If $\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is continuous, irreducible and totally odd, then there exists a Hilbert modular eigenform f such that $\rho \cong \overline{\rho}_f$.*

(Totally odd means that $\det \rho(c) = -1$ for each of the $[F : \mathbf{Q}]$ complex conjugations in $\mathrm{Gal}(\overline{F}/F)$.) The issue at hand is how to make this precise: what are the possible weights and levels of the Hilbert modular forms associated to ρ? We note that, since the weight of a Hilbert modular form is a a tuple of integers, there is already no natural definition of a minimal weight available anymore. To make matters worse it turns out that the notions of level and weight become intertwined. Lastly, it turns out that one can use a simple argument using determinants (see [BDJ10, §1]) that unlike the $F = \mathbf{Q}$ case not all mod p Galois representations as above arise as the reduction of a Hilbert modular eigenform of level prime-to-p; in particular, the conjecture as we have set it up here will not hold. Instead we should have used automorphic forms with mod p coefficients.

3.2.1.1. *The Buzzard–Diamond–Jarvis approach.* These issues are met in the paper of Buzzard, Diamond and Jarvis by introducing modularity via Serre weights. We will sketch their approach here following [Sch13, §2.3].

DEFINITION 3.2.2. A **Serre weight** for F is an isomorphism class of irreducible $\overline{\mathbf{F}}_p$-representations of the group $\mathrm{GL}_2(\mathcal{O}_F/p\mathcal{O}_F) = \prod_{\mathfrak{p}|p} \mathrm{GL}_2(\mathcal{O}_F/\mathfrak{p})$, where $\mathcal{O}_F$ denotes the ring of integers of F and the product runs over all primes of $\mathcal{O}_F$ dividing p.

Therefore, the (global) Serre weights for F are of the form $V = \otimes_{\mathfrak{p}|p} V_{\mathfrak{p}}$, where the tensor product is over $\overline{\mathbf{F}}_p$ and each $V_{\mathfrak{p}}$ is an irreducible $\overline{\mathbf{F}}_p$-representation of $\mathrm{GL}_2(\mathcal{O}_F/\mathfrak{p})$. These can be described explicitly as follows.

DEFINITION 3.2.3. Suppose K is a finite extension of $\mathbf{Q}_p$ with residue field k. A **Serre weight** for K is an irreducible $\overline{\mathbf{F}}_p$-representation of $\mathrm{GL}_2(k)$, which is necessarily of the form

$$V_{\underline{a},\underline{b}} := \bigotimes_{\lambda \in \mathrm{Hom}(k, \overline{\mathbf{F}}_p)} (\det{}^{b_\lambda} \otimes_k \mathrm{Sym}^{a_\lambda - b_\lambda} k^2) \otimes_{k,\lambda} \overline{\mathbf{F}}_p$$

for some uniquely determined integers a_λ, b_λ with $b_\lambda, a_\lambda - b_\lambda \in [0, p-1]$ for all λ and $b_\lambda < p-1$ for at least one λ.

Let D/F be a quaternion algebra that splits at exactly one real place of F and at all places above p. Since we impose no requirements at the other places, there are no parity issues. In other words, we have isomorphisms

$$D \otimes_{\mathbf{Q}} \mathbf{R} \cong M_2(\mathbf{R}) \times \mathbb{H}^{d-1};$$
$$D \otimes_{\mathbf{Q}} \mathbf{Q}_p \cong M_2(F \otimes_{\mathbf{Q}} \mathbf{Q}_p).$$

Letting $\mathbb{A}_{F,f}$ denote the finite adèles of F (and, similarly, $\mathbb{A}_{\mathbf{Q},f}$ for the finite adèles of $\mathbf{Q}$), we define a compact open subgroup $U \subset (D \otimes_F \mathbb{A}_{F,f})^\times$ as follows. We take $U^p \subset (D \otimes_F \mathbb{A}^p_{F,f})^\times$ to be any compact open subgroup and define $U_p \subset (D \otimes_F \mathbb{A}_{F,p})^\times$ via

$$U_p := \prod_{\mathfrak{p}|p} \ker\left(\mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}}) \to \mathrm{GL}_2(f_\mathfrak{p})\right),$$

where $\mathcal{O}_{F_\mathfrak{p}}$ denotes the ring of integers of the completion of F at a prime ideal $\mathfrak{p}$ and $f_\mathfrak{p}$ denotes the residue field of this local ring. We define $U := U^p \times U_p$.

Denoting $G := \mathrm{Res}_{F/\mathbf{Q}} D^\times$, the Shimura curve S_U with complex valued points

$$S_U(\mathbf{C}) = G(\mathbf{Q}) \backslash \left(G(\mathbb{A}_{\mathbf{Q},f}) \times \mathcal{H}^\pm\right)/U$$

has a (canonical) model over F. We let $W \subset G(\mathbb{A}_{\mathbf{Q},f}) = (D \otimes_F \mathbb{A}_{F,f})^\times$ be the open compact subgroup defined by

$$W = U^p \times \left(\prod_{\mathfrak{p}|p} \mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}})\right).$$

If U^p is sufficiently small (see [BDJ10, p. 7]), then the natural map $S_U \to S_W$ is a Galois cover of Shimura curves with Galois group $W/U \cong \prod_{v|p} \mathrm{GL}_2(f_\mathfrak{p})$. Then W/U acts naturally on the right on S_U, and, hence, naturally on the left on $\mathrm{Pic}^0(S_U)$ and $\mathrm{Pic}^0(S_U)[p](\overline{K})$.

Definition 3.2.4. Let F be a totally real field and let V be a Serre weight for F. Moreover, let $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ be a continuous, irreducible representation. Then we say ρ is **modular of Serre weight V** if there exists a quaternion algebra D/F and an open compact subgroup $U \subset (D \otimes_F \mathbb{A}_{F,f})^\times$ as above such that ρ is an $\overline{\mathbf{F}}_p[G_F]$-submodule of

$$\left(\mathrm{Pic}^0(S_U)[p](\overline{K}) \otimes V\right)^{\prod_{\mathfrak{p}|p} \mathrm{GL}_2(f_\mathfrak{p})},$$

where $\mathrm{GL}_2(\mathcal{O}_F/p\mathcal{O}_F) = \prod_{\mathfrak{p}|p} \mathrm{GL}_2(f_\mathfrak{p})$ acts diagonally on the tensor product and G_F acts trivially on V.

We note that it is proved in [BDJ10, Lem. 2.4] that the above definition is equivalent to ρ being an $\overline{\mathbf{F}}_p[G_F]$-submodule of $H^1_{\text{ét}}(S_{W,\overline{F}}, \mathcal{F}_{V(1)})$, where, for any finite-dimensional $\overline{\mathbf{F}}_p$-vector space V with a left W/U-action, the sheaf $\mathcal{F}_V$ is (the pullback to $S_{W,\overline{F}}$ of) some locally constant étale sheaf on S_W with the property that the pullback to S_U is just the constant sheaf associated to V. This definition looks more like the definitions we saw in the previous chapter.

In [BDJ10, §2] there is an extensive discussion linking this definition of modularity to the usual definition in terms of reductions of Galois representations coming from a Hilbert modular form. In particular, let us quote the following result. Let Σ_F denote the embeddings $F \hookrightarrow \mathbf{R}$ and let $\Sigma_\mathfrak{p}$ denote the embeddings $f_\mathfrak{p} \hookrightarrow \overline{\mathbf{F}}_p$.

PROPOSITION 3.2.5. *Let $(\underline{k}, w) \in \mathbf{Z}_{\geqslant 2}^{\Sigma_F} \times \mathbf{Z}$ be integers all of the same parity. Suppose $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is continuous, irreducible and totally odd. Then $\rho \sim \overline{\rho}_f$ for some (possibly non-classical) holomorphic Hilbert modular form f of weight $(\underline{k}, w)$ and of level prime to p if and only if ρ is modular of weight V for some Jordan–Hölder constituent V of*

$$\bigotimes_{\mathfrak{p}|p} \bigotimes_{\sigma\in\Sigma_\mathfrak{p}} \det{}^{(w-k_\sigma)/2} \otimes \mathrm{Sym}^{k_\tau-2} f_\mathfrak{p}^2 \otimes_{f_\mathfrak{p},\sigma} \overline{\mathbf{F}}_p.$$

PROOF. This is [BDJ10, Prop. 2.5]. □

3.2.1.2. *Sets of associated weights.* Given a continuous irreducible representation $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ the next goal is to write down a complete set of Serre weights V for F such that ρ is modular of weight V. We will denote this set by $W(\rho)$.

The first important property of the set $W(\rho)$ is that it is defined completely locally. This means that for any prime ideal $\mathfrak{p} \mid p$ we will define a set $W(\rho|_{G_{F_\mathfrak{p}}})$ of (local) Serre weights for the field $F_\mathfrak{p}$ associated to the local representation $\rho : G_{F_\mathfrak{p}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$. The set $W(\rho)$ of global Serre weights is then defined as

$$W(\rho) := \left\{ V = \bigotimes_{\mathfrak{p}|p} V_\mathfrak{p} \;\middle|\; V_\mathfrak{p} \in W(\rho|_{G_{F_\mathfrak{p}}}) \text{ for all } \mathfrak{p} \mid p \right\}.$$

This feature of the set of associated weights $W(\rho)$ will allow us to work locally. Another important property is that the sets of associated weights will be determined completely by their restriction to inertia meaning that $W(\rho|_{G_{F_\mathfrak{p}}}) := W(\rho|_{I_{F_\mathfrak{p}}})$ by definition.

Let us fix a prime $\mathfrak{p} \mid p$. Suppose the local field $F_\mathfrak{p}$ has ramification index $e_\mathfrak{p}$. Denote the residue field by $f_\mathfrak{p}$. We let $F'_\mathfrak{p}/F_\mathfrak{p}$ denote the quadratic unramified extension of $F_\mathfrak{p}$ and its residue field by $f'_\mathfrak{p}$.

The following definition appeared first in [Sch08] in full generality (building on previous results of [BDJ10] for $e_\mathfrak{p} = 1$).

DEFINITION 3.2.6. If $\rho|_{G_{F_\mathfrak{p}}}$ is irreducible, then a Serre weight $V_{\underline{a},\underline{b}}$ (as in Definition 3.2.3) is in $W(\rho|_{G_{F_\mathfrak{p}}})$ if and only if there is a set $J \subset \mathrm{Hom}(f'_\mathfrak{p}, \overline{\mathbf{F}}_p)$ consisting of exactly one embedding extending each element of $\mathrm{Hom}(f_\mathfrak{p}, \overline{\mathbf{F}}_p)$ and for each $\sigma \in \mathrm{Hom}(f_\mathfrak{p}, \overline{\mathbf{F}}_p)$ an integer $0 \leqslant \delta_\sigma \leqslant e_\mathfrak{p} - 1$ such that if we write $\mathrm{Hom}(f'_{\mathfrak{p}}, \overline{\mathbf{F}}_p) = J \coprod J^c$, then $\rho|_{I_{F_{\mathfrak{p}}}}$ is isomorphic to

$$\begin{pmatrix} \prod_{\sigma\in J}\omega_\sigma^{a_\sigma+1+\delta_\sigma}\prod_{\sigma\in J^c}\omega_\sigma^{b_\sigma+e_{\mathfrak{p}}-1-\delta_\sigma} & 0 \\ 0 & \prod_{\sigma\in J^c}\omega_\sigma^{a_\sigma+1+\delta_\sigma}\prod_{\sigma\in J}\omega_\sigma^{b_\sigma+e_{\mathfrak{p}}-1-\delta_\sigma} \end{pmatrix},$$

where, by abuse of notation, we have written δ_σ for $\delta_{\sigma|f_{\mathfrak{p}}}$ and the characters ω_σ are the fundamental characters defined in the introduction.

It is well known (see, for example, [Sch08, pp. 8–7]) that if $\rho|_{G_{F_{\mathfrak{p}}}}$ is irreducible, then

$$\rho|_{I_{F_{\mathfrak{p}}}} \cong \begin{pmatrix} \chi & 0 \\ 0 & \chi' \end{pmatrix}$$

for characters $\chi, \chi' : I_{F_{\mathfrak{p}}} \to \overline{\mathbf{F}}_p^\times$ factoring through $(f'_{\mathfrak{p}})^\times$ such that $\chi^{q_{\mathfrak{p}}} = \chi'$ and $(\chi')^{q_{\mathfrak{p}}} = \chi$ for $q_{\mathfrak{p}} := |f_{\mathfrak{p}}|$. The definition above clearly satisfies this requirement.

We will give more details for the locally reducible case in the next section, but let us sketch the approach.

Definition 3.2.7. If $\rho|_{G_{F_{\mathfrak{p}}}}$ is reducible, then $\rho|_{I_{F_{\mathfrak{p}}}}$ is of the form

$$\rho|_{I_{F_{\mathfrak{p}}}} \cong \begin{pmatrix} \chi_1 & *_\rho \\ 0 & \chi_2 \end{pmatrix}$$

for two characters $\chi_1, \chi_2 : I_{F_{\mathfrak{p}}} \to \overline{\mathbf{F}}_p^\times$. The $*_\rho$ then defines an extension class in $H^1(G_{F_{\mathfrak{p}}}, \overline{\mathbf{F}}_p(\chi))$, where $\chi := \chi_1\chi_2^{-1}$. For a given Serre weight $V_{\underline{a},\underline{b}}$ we define a subspace $L_{V_{\underline{a},\underline{b}}} \subseteq H^1(G_{F_{\mathfrak{p}}}, \overline{\mathbf{F}}_p(\chi))$ in terms of crystalline lifts. Then we define

$$V_{\underline{a},\underline{b}} \in W(\rho) \text{ if and only if } *_\rho \in L_{V_{\underline{a},\underline{b}}}.$$

We remark that the definition of the set $W(\rho)$ is completely explicit in the case that the local representation at $\mathfrak{p}$ is irreducible. However, in the locally reducible case these spaces $L_{V_{\underline{a},\underline{b}}}$ appear, which are defined inexplicitly in terms of p-adic Hodge theory (see §3.3 for a precise definition). Therefore, if our goal is to obtain an explicit version of the Buzzard–Diamond–Jarvis conjecture and its extensions, then we may focus on the locally reducible case and try to give a different more explicit description of these distinguished subspaces. This is what we will do in the remainder of this thesis.

For completeness we state the full strong modularity conjecture for mod p Hilbert modular forms.

Conjecture 3.2.8. *Let F be a totally real field. If $\rho : G_F \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is continuous, irreducible and totally odd, then ρ is modular. Moreover, if*

V is a Serre weight for F, then ρ is modular of weight V if and only if $V \in W(\rho)$.

A precise statement of this conjecture was first given in [BDJ10] under the assumption that p is unramified in F and it was subsequently extended by Schein [Sch08] and by Gee and co-authors (see [BLGG13, §4] for a good overview). The so-called weight part of the conjecture (i.e. if ρ is modular then it must be modular of the predicted weights) has been proved in [GLS15] building on previous work of Gee and co-authors. However, little is currently known towards a full proof of the conjecture.

3.3. The distinguished subspaces L_V

Having explained our motivation coming from the global conjecture of Buzzard, Diamond and Jarvis [BDJ10] and its extensions (see [BLGG13, §4]), we will now focus our attention on the locally residually reducible case: the only case in which the several conjectures are not completely explicit yet. Therefore, we may restrict our global representation to a decomposition group at a prime above p and work locally from now on. In this section we will give a precise description in terms of p-adic Hodge theory of the weight conjecture in the locally residually reducible case following [GLS15, §4]. This is the description as given in the original conjectures.

3.3.1. Extension classes. Let p be any prime and let K be a finite extension of $\mathbf{Q}_p$ with residue degree f, ramification degree e and residue field k. Suppose that $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is a reducible representation, i.e. we can write

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix} \tag{3.3.1}$$

for some characters $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$. Writing $\chi := \chi_1\chi_2^{-1}$ the representation ρ defines an extension class in $\mathrm{Ext}_{\overline{\mathbf{F}}_p[G_K]}(\overline{\mathbf{F}}_p, \overline{\mathbf{F}}_p(\chi)) = H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ in the following way: after twisting we obtain

$$\chi_2^{-1} \otimes \rho \sim \begin{pmatrix} \chi & c_\rho \\ 0 & 1 \end{pmatrix},$$

where c_ρ is now a cocycle in $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$, which is well-defined up to a scalar in $\overline{\mathbf{F}}_p^\times$ (in the sense that choosing a different basis for which ρ is of the form of Equation 3.3.1 will give a non-zero scalar multiple of c_ρ). We will associate the class of c_ρ to ρ. Since we are now working locally, we may use the explicit description of Definition 3.2.3 to define our Serre weights V as irreducible $\overline{\mathbf{F}}_p$-representations of $\mathrm{GL}_2(k)$.

We will say that "ρ is modular of a certain Serre weight V" if the class $c_\rho \in H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ lies in a certain subspace of extensions depending on V and ρ (or, more precisely, on its semisimplification ρ^{ss}) – strictly speaking it may not always be a subspace as it is possible that is empty. We will now define this 'distinguished subspace'.

3.3.2. Extensions of crystalline characters. Given an ordered pair of mod p characters (χ_1, χ_2) of G_K and a Serre weight $V_{\underline{a},\underline{b}}$ as in Definition 3.2.3, we would like to define a subspace $L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2) \subset H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. To simplify our notation let us write a_i and b_i for $a_{\overline{\tau}_i}$ and $b_{\overline{\tau}_i}$. Recall that for each $\tau \in \mathrm{Hom}_{\mathbf{Q}_p}(K, \overline{\mathbf{Q}}_p)$ any crystalline character $\tilde{\chi} : G_K \to \overline{\mathbf{Q}}_p^{\times}$ has a unique τ-labelled Hodge-Tate weight m_τ and together these define $\tilde{\chi}$ up to an unramified character. Similarly, a 2-dimensional crystalline representation $\tilde{\rho} : G_K \to \mathrm{GL}_2(\overline{\mathbf{Q}}_p)$ has two unique, possibly equal, τ-labelled Hodge-Tate weights m_τ and m'_τ. The set of τ-labelled Hodge-Tate weights is always denoted by $\mathrm{HT}_\tau(\tilde{\rho})$. Recall our definition of the embeddings $\tau_{i,j}$ in §1.1.

DEFINITION 3.3.1. We say that a crystalline representation $\tilde{\rho}$ has **Hodge type** $(\underline{a}, \underline{b})$ if $\mathrm{HT}_{\tau_{i,0}}(\tilde{\rho}) = \{b_i, a_i + 1\}$ and $\mathrm{HT}_{\tau_{i,j}}(\tilde{\rho}) = \{0, 1\}$ for $j > 0$.

DEFINITION 3.3.2. Following the nomenclature of Gee–Liu–Savitt (see [GLS15]) we will say that a representation is **pseudo-Barsotti–Tate of weight** $\{a_i + 1\}$, or simply **pseudo-BT**, if it has Hodge type $(\underline{a}, \underline{0})$. To simplify the notation we will refer to the weight of such a representation as $\{r_i\}$, where $r_i := a_i + 1 \in [1, p]$.

DEFINITION 3.3.3. For any ordered pair of characters $\chi_1, \chi_2 \colon G_K \to \overline{\mathbf{F}}_p^{\times}$ and a Serre weight $V_{\underline{a},\underline{b}}$, let the **distinguished subspace** $L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2)$ be defined as the subset obtained as the reduction of all crystalline representations of Hodge type $(\underline{a}, \underline{b})$ of the form

$$\begin{pmatrix} \tilde{\chi}_1 & * \\ 0 & \tilde{\chi}_2 \end{pmatrix},$$

where $\tilde{\chi}_1$ and $\tilde{\chi}_2$ are any crystalline lifts of χ_1 and χ_2, respectively.

Note that if ψ is any such reduction then ψ is an $\overline{\mathbf{F}}_p[G_K]$-extension of $\overline{\mathbf{F}}_p(\chi_2)$ by $\overline{\mathbf{F}}_p(\chi_1)$ and we get a cohomology class $z_\psi \in H^1(G_K, \mathbf{F}_p(\chi))$

associated to ψ, for example, by considering

$$\chi_2^{-1} \otimes \psi \sim \begin{pmatrix} \chi & z_\psi \\ 0 & 1 \end{pmatrix}.$$

A priori it is not clear that this always defines a subspace of the $\overline{\mathbf{F}}_p$-space $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ rather than just a subset. Indeed, it turns out that with the definition as above it is possible that $L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2)$ is empty and, hence, not a subspace. However, as long as $L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2)$ is non-empty, it turns out that it will always be a subspace (this follows, for example, from the results of [GLS15]).

For a reducible representation $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ of the form

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

we will denote the set of Serre weights V for which ρ is 'modular of weight V' by $W(\rho)$. This leads to the following definition.

Definition 3.3.4. For any Serre weight V, we define

$$V \in W(\rho) \iff c_\rho \in L_V(\chi_1, \chi_2).$$

It follows from the definitions that

$$L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2) = L_{V_{\underline{a}-\underline{b},\underline{0}}}(\prod_i \omega_i^{-b_i} \otimes \chi_1, \prod_i \omega_i^{-b_i} \otimes \chi_2).$$

Hence, if necessary, we may freely assume that the determinant in our Serre weights is trivial, or, equivalently, we need only consider crystalline lifts in Definition 3.3.3 that are pseudo-Barsotti Tate.

We remark that the definition that we have used here for the distinguished subspaces will lead to what in the literature is often referred to as $W^{\text{explicit}}(\rho)$. However, in [GLS15] it is proved that this way of defining the distinguished subspaces is equivalent to others such as $W^{\mathrm{BT}}(\rho)$ or $W^{\text{cris}}(\rho)$. We have chosen the definition that seemed most natural to us. One of the main goals of this thesis is to find a more explicit description of the spaces $L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2)$ without making use of the advanced machinery of p-adic Hodge theory.

CHAPTER 4

The peu ramifié subspace

In this chapter we will prove an interesting and useful result which is known to experts but for which (as far as we are aware) there is no good reference available: we will prove that the distinguished subspaces L_V are always contained in the so-called peu ramifié subspace. Beyond the clear benefit of having a proof of this result publicly available we also need this result in the upcoming arguments. Therefore, it seemed appropriate to include a full discussion here. We have tried to keep this chapter reasonably self-contained meaning it can be read without too much reference to earlier or later parts of the thesis.

4.1. Introduction

Firstly, let us briefly recall our notation and introduce new notation where necessary. Let p be a prime. Suppose $K/\mathbf{Q}_p$ is a finite extension of local fields of ramification degree e and residue degree f. We write k for the residue field of K and K_0 for the maximal unramified subextension. We fix a uniformiser $\pi_K \in K$. If $p = 2$, we make sure our uniformiser satisfies [Wan17, Lem. 2.1] (see §1.1). Let E denote a sufficiently large finite extension of $\mathbf{Q}_p$ such that the images of all embeddings of K and its quadratic unramified extension are contained in E and so that all our crystalline representations are defined over E. Denote its residue field by k_E. We fix an element $\tau_0 \in \mathrm{Hom}_{\mathbf{Q}_p}(K_0, E)$, and recursively define $\tau_i \in \mathrm{Hom}_{\mathbf{Q}_p}(K_0, E)$ for $i \in \mathbf{Z}$ so that $\tau_{i+1}^p \equiv \tau_i \bmod p$. Then the elements of $\mathrm{Hom}_{\mathbf{Q}_p}(K_0, E)$ are given by $\tau_0, \ldots, \tau_{f-1}$. Now label the elements of $\mathrm{Hom}_{\mathbf{Q}_p}(K, E)$ as

$$\mathrm{Hom}_{\mathbf{Q}_p}(K, E) = \{\tau_{i,j} : i = 0, \ldots, f-1 \text{ and } j = 0, \ldots, e-1\}$$

in any way such that $\tau_{i,j}|_{K_0} = \tau_i$. Recall, moreover, that we have a character $\overline{\omega}_{\mathrm{fc}} : G_K \to k^\times$ defined by $\overline{\omega}_{\mathrm{fc}}(g) = g(\pi)/\pi$, where π is a root of $x^{p^f-1} + \pi_K = 0$. We define $\omega_i : G_K \to \overline{\mathbf{F}}_p^\times$, the **fundamental characters of level f**, as $\omega_i := \overline{\tau}_i \circ \overline{\omega}_{\mathrm{fc}}$ for $i = 0, \ldots, f-1$. We let $c \in \overline{\mathbf{F}}_p^\times$ denote the element obtained as follows: we write the mod p cyclotomic character as $\varepsilon = \mu \cdot \prod_i \omega_i^e$ for an unramified character μ and we let $c := \mu(\mathrm{Frob}_K)$.

Recall that a **Serre weight** of $\mathrm{GL}_2(k)$ is an irreducible $\overline{\mathbf{F}}_p$-representation of $\mathrm{GL}_2(k)$, which must be of the form

$$V_{a,b} := \bigotimes_{\lambda \in \mathrm{Hom}_{\mathbf{F}_p}(k, \overline{\mathbf{F}}_p)} \det{}^{b_\lambda} \otimes \mathrm{Sym}^{a_\lambda - b_\lambda} k^2 \otimes_{k,\lambda} \overline{\mathbf{F}}_p,$$

for some uniquely determined integers a_λ, b_λ with $b_\lambda, a_\lambda - b_\lambda \in [0, p-1]$ for all λ, and not all b_λ equal to $p-1$. Note that we may replace $\overline{\mathbf{F}}_p$ in the definition above by k_E, which will be convenient for us. We will also write a_i and b_i for $a_{\overline{\tau}_i}$ and $b_{\overline{\tau}_i}$, respectively.

4.1.1. The subspaces $L_{V_{\underline{a},\underline{b}}}$. We recall briefly certain definitions from §3.3. Suppose $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is a reducible continuous representation such that

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix},$$

where $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$ are continuous characters. Write $\chi := \chi_2^{-1}\chi_1$ for the quotient of the characters. We say that a de Rham lift $\tilde{\rho}$ of ρ has **Hodge type** $(\underline{a}, \underline{b})$ if $\mathrm{HT}_{\tau_{i,0}}(\tilde{\rho}) = \{b_i, a_i + 1\}$ for $0 \leqslant i \leqslant f-1$ and $\mathrm{HT}_{\tau_{i,j}}(\tilde{\rho}) = \{0, 1\}$ for $j > 0$. Note that a crystalline representation of Hodge type $(\underline{1}, \underline{0})$ is Barsotti–Tate and we will refer to a crystalline representation of Hodge type $(\underline{a}, \underline{0})$ as a **pseudo-BT representation of weight** $\{a_i + 1\}$. In this case we will sometimes write $r_i := a_i + 1 \in [1, p]$.

For any Serre weight $V_{\underline{a},\underline{b}}$ we defined a subset of extensions

$$L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2) \subset H^1(G_K, \overline{\mathbf{F}}_p(\chi))$$

as the subset of all extensions which arise as the reduction of a crystalline representation of Hodge type $(\underline{a}, \underline{b})$ of the form

$$\begin{pmatrix} \tilde{\chi}_1 & * \\ 0 & \tilde{\chi}_2 \end{pmatrix}$$

for any crystalline lifts $\tilde{\chi}_1$ and $\tilde{\chi}_2$ of χ_1 and χ_2, respectively.

We can compute that $L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2) = L_{V_{\underline{a}-\underline{b},\underline{0}}}(\prod_i \omega_i^{-b_i} \otimes \chi_1, \prod_i \omega_i^{-b_i} \otimes \chi_2)$, hence we can always reduce to the pseudo-BT case. More generally, if $\xi : G_K \to \overline{\mathbf{F}}_p^\times$ is any continuous character such that $\xi|_{I_K} = \prod_i \omega_i^{c_i}$ and we write $\xi \otimes V_{\underline{a},\underline{b}}$ for the Serre weight $V_{\underline{\tilde{a}},\underline{\tilde{b}}}$ with indices $\tilde{a}_i = a_i + c_i$ and $\tilde{b}_i = b_i + c_i$, then it follows immediately from the definitions that

$$L_{\xi \otimes V_{\underline{a},\underline{b}}}(\xi\chi_1, \xi\chi_2) = L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2).$$

Hence, twisting does not change the subspace of extensions under consideration. In particular, we are free to twist our representations by a character without changing the space of extensions.

By the results of [Wan17] (since we have carefully chosen our uniformiser) the results quoted from [GLS15] carry over immediately to $p = 2$ and we will stop mentioning this explicitly in the remainder of this chapter.

4.1.2. The peu ramifié subspace. From now on we will assume that the character χ is the mod p cyclotomic character. We will also assume that if $r_i := a_i + 1 = p$ for all i then χ_2 is ramified. (The remaining case is an exceptional case that has to be treated separately.) Recall that if χ is cyclotomic, then Kummer theory allows us to write down an isomorphism $H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \cong K^\times \otimes \overline{\mathbf{F}}_p$. By definition, the **peu ramifié subspace** of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ is the codimension-one subspace of classes that correspond to elements of $\mathcal{O}_K^\times \otimes \overline{\mathbf{F}}_p$. Let us write $H^1_{\mathrm{pr}}(G_K, \overline{\mathbf{F}}_p(\chi))$ for the peu ramifié subspace of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. Any element of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ that is in the complement of the peu ramifié subspace will be called **très ramifié**. Note that the collection of très ramifiées classes is not a subspace. However, if we choose any uniformiser $\pi \in K$, then π spans a so-called **très ramifiée line** $\langle \pi \cdot (K^\times)^p \rangle \subset K^\times/(K^\times)^p$. The union of all these lines (minus the identity element) gives all très ramifiées classes.

4.1.3. The statement. We can now state the main theorem of this chapter.

Theorem 4.1.1. *Suppose that $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$ are two characters such that the quotient of the characters $\chi := \chi_2^{-1}\chi_1$ is the mod p cyclotomic character and let $V_{\underline{a},\underline{b}}$ be a Serre weight. Suppose, moreover, that if χ_2 is unramified, then $r_i := a_i - b_i + 1 < p$ for at least one i (i.e. we will exclude the exceptional case above). Then we have that*

$$L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2) \subset H^1_{\mathrm{pr}}(G_K, \overline{\mathbf{F}}_p(\chi)).$$

In fact, if χ is the mod p cyclotomic character then, in the exceptional case when χ_2 is unramified and $r_i = p$ for all i, it turns out that

$$L_{V_{\underline{p-1},\underline{0}}}(\chi, \mathbf{1}) = H^1(G_K, \overline{\mathbf{F}}_p(\chi)).$$

Therefore the non-exceptional condition in the statement of the result above is necessary. The cyclotomic condition is needed, of course, because the peu ramifié subspace is only defined when the quotient of the characters is cyclotomic.

We will prove this theorem by proving the following two propositions.

PROPOSITION 4.1.2. *Let χ be the mod p cyclotomic character. Then, for the distinguished subspace associated to the trivial Serre weight $V_{\underline{0},\underline{0}}$, we find that*

$$L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1}) = H^1_{\mathrm{pr}}(G_K, \overline{\mathbf{F}}_p(\chi)).$$

PROPOSITION 4.1.3. *Suppose that $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$ are two characters such that the quotient of the characters $\chi := \chi_2^{-1}\chi_1$ is the mod p cyclotomic character and let $V_{\underline{a},\underline{b}}$ be a Serre weight. Suppose, moreover, that if χ_2 is unramified, then $a_i - b_i + 1 < p$ for at least one i. Then*

$$L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2) \subset L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1}).$$

REMARK 4.1.4. Toby Gee rightly points out to us that an alternative proof of Theorem 4.1.1 for $p > 2$ is given by [CEGS19, Lem. B5].

4.2. The trivial Serre weight case

In this section we would like to prove Proposition 4.1.2. We will use some techniques from the proof of Theorem 5.4.1 [GLS15, p. 34]. Let us first note that we are free to use the techniques of that proof even though we are in the cyclotomic case (the proof assumes χ not cyclotomic) since it follows from the proof of Theorem 6.1.8 [GLS15, p. 38] that in the non-exceptional case the restriction map $H^1(G_K, \mathbf{F}_p(\chi)) \to H^1(G_{K_\infty}, \mathbf{F}_p(\chi))$ is still injective when restricted to $L_{V_{\underline{a},\underline{0}}}(\chi_1, \chi_2)$. The injectivity of this map when restricted to one of the subspaces is the only place in the proof of Theorem 5.4.1 where χ being non-cyclotomic is used.

In Proposition 4.1.2 we are considering the subspace $L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1})$, where χ denotes the mod p cyclotomic character. Since we consider the trivial Serre weight $V_{\underline{0},\underline{0}}$, we are considering extension classes that arise as the reduction of a pseudo-BT representation of parallel weight $r_i = 1$ for all i (i.e. a Barsotti–Tate representation) of the right form.

Let $\tilde{\chi}_p$ denote the usual p-adic cyclotomic character $\tilde{\chi}_p : G_K \to \mathbf{Z}_p^\times$. It follows from the proof of Theorem 5.4.1 [GLS15, p. 33] that the image of $H^1_f(G_K, \mathcal{O}_E(\tilde{\chi}_p))$ in $H^1(G_K, k_E(\chi))$, which is equal to $L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1})$ by the same proof, has dimension ef unless χ is also trivial in which case it has dimension $ef + 1$. Either way it follows that $L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1}) \subset H^1(G_K, k_E(\chi))$ is a subspace of codimension 1; recall that the k_E-dimension of $H^1(G_K, k_E(\chi))$ is $ef + 1$ if χ is cyclotomic and non-trivial and $ef + 2$ if χ is also trivial. Since we already know that

$$H^1_{\mathrm{pr}}(G_K, k_E(\chi)) \subset H^1(G_K, k_E(\chi))$$

is also a subspace of codimension 1, it is enough to give one inclusion between $L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1})$ and $H^1_{\mathrm{pr}}(G_K, k_E(\chi))$ to show equality.

In the remainder of this section, we will do a bit of work to prove the inclusion $L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1}) \subseteq H^1_{\mathrm{pr}}(G_K, k_E(\chi))$. However, Laurent Berger cleverly points out to us that it is shorter to prove $H^1_{\mathrm{pr}}(G_K, k_E(\chi)) \subseteq L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1})$ using Alain Muller's PhD thesis [Mul13]. Indeed, it is proved in [Mul13, Prop. 2.5.6] that a reducible representation corresponding to a class in $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ which is *peu ramifiée* lifts to a crystalline extension of the trivial character by the cyclotomic character. This crystalline extension must therefore correspond to an element of $H^1_f(G_K, \mathcal{O}_E(\tilde{\chi}_p))$ whose image in $H^1(G_K, k_E(\chi))$ equals $L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1})$ as noted above. Since we believe Proposition 4.2.1 and its proof to be interesting in its own right, we will now return to our original approach.

By a theorem of Breuil [Bre00, Thm. 1.4] (and Kisin [Kis06, Cor. 2.2.6] for $p = 2$) any representation V in $H^1_f(G_K, E(\tilde{\chi}_p))$ (i.e. a crystalline representation of G_K that arises as an extension of the trivial character by $\tilde{\chi}_p$) comes from a Barsotti–Tate group Γ over $\mathcal{O}_K$ via $V \cong T_p\Gamma \otimes E$. It follows from this theorem that any representation in the image of $H^1_f(G_K, \mathcal{O}_E(\tilde{\chi}_p))$ in $H^1(G_K, k_E(\chi))$ arises as the reduction of the Tate module of a Barsotti–Tate group, hence as a finite flat group scheme.

Proposition 4.2.1. *An element of $H^1(G_K, k_E(\chi))$ coming from a finite flat group scheme is peu ramifié, i.e. it is an element of $H^1_{\mathrm{pr}}(G_K, k_E(\chi))$.*

This is proved by Edixhoven [Edi92, Prop. 8.2] in the case $K = \mathbf{Q}_p$ using an *fppf* Kummer theory argument. It may be possible to extend his argument to any finite extension K of $\mathbf{Q}_p$, but instead we will give a different proof here.

Proof. We will prove that if an element is très ramifié then it cannot come from a finite flat group scheme.

The first thing to note is that we may assume that K contains a pth root of unity ζ_p. If not, then define $L := K(\zeta_p)$ which is an extension of K of degree $d \mid p-1$. We claim that any class that is très ramifié for K is also très ramifié for L. If we write $\iota : K \to L$ for the field inclusion, then we have commuting exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p & \hookrightarrow & K^\times/(K^\times)^p & \xrightarrow{v_K} & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \cdot d} & & \\ 1 & \longrightarrow & \mathcal{O}_L^\times/(\mathcal{O}_L^\times)^p & \hookrightarrow & L^\times/(L^\times)^p & \xrightarrow{v_L} & \mathbf{Z}/p\mathbf{Z} & \longrightarrow & 0. \end{array}$$

The très ramifiés elements for K are exactly those that are not in the kernel of the map v_K. Since multiplication by d is an isomorphism, we see that $x \cdot (K^\times)^p$ is not in the kernel of v_K if and only if $\iota(x) \cdot (L^\times)^p$ is not in the kernel of v_L. So x is très ramifié if and only if $\iota(x)$ is très ramifié for L. Therefore, we may assume without loss of generality that $\zeta_p \in K$.

First we use Kummer theory and local class field theory to translate the problem into explicit language. Suppose that we choose a uniformiser $\pi \in K$. Write μ_p for the pth roots of unity in K with their Galois action. By Kummer theory we have correspondences

$$\begin{tikzcd}
K^\times/(K^\times)^p \arrow[r, leftrightarrow, "\sim"] & \mathrm{Hom}_{\mathrm{cont}}(G_K, \mu_p) \\
\langle \pi \cdot (K^\times)^p \rangle \arrow[u, hook] \arrow[r, leftrightarrow, "\sim"] & \mathrm{Hom}(\mathrm{Gal}(M/K), \mu_p), \arrow[u, hook]
\end{tikzcd}$$

where $M := K(\pi^{1/p})$ is obtained by adjoining a pth root of π. The inclusion on the right is given via the map $G_K \twoheadrightarrow \mathrm{Gal}(M/K) \to \mu_p$. As explained above the très ramifiées classes are given by the union of the très ramifiés lines of the form $\langle \pi \cdot (K^\times)^p \rangle$ for a uniformiser π of K. Since for any $f : G_K \to \mu_p$ we have that $\ker(f)$ must be G_K or the absolute Galois group of a size p extension of K, we see that a continuous homomorphism $f : G_K \to \mu_p$ is très ramifié if and only if there exists a uniformiser π of K such that $\ker(f) = G_M$ for $M := K(\pi^{1/p})$.

Using local class field theory, we see that the diagram

$$\begin{tikzcd}
G_K \arrow[rr] \arrow[dr, two heads] & & \mu_p \\
& \mathrm{Gal}(M/K) \arrow[ur] &
\end{tikzcd}$$

becomes

$$\begin{tikzcd}
K^\times \arrow[rr] \arrow[dr, two heads] & & \mu_p \\
& K^\times/N_{M/K}(M^\times). \arrow[ur] &
\end{tikzcd}$$

We see that f is très ramifié if and only if $\ker(f) = N_{M/K}(M^\times)$ for an extension M as above.

Suppose now that $f \in H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \cong K^\times/(K^\times)^p \cong \mathrm{Hom}_{\mathrm{cont}}(G_K, \mu_p)$ arises as G_K acting on $\Gamma(\overline{K})$ for a Γ a finite flat group scheme over $\mathcal{O}_K$ killed by p. It then follows by a theorem from Fontaine [Fon85, Thm. A] that the restriction of f to $G_K^{\frac{ep}{p-1}}$ is trivial. In other words, $\ker(f) \supseteq G_K^{\frac{ep}{p-1}}$. Note that $p - 1 \mid e$ since we assume $\zeta_p \in K$. By local class field theory the higher ramification group $G_K^{\frac{ep}{p-1}}$ is mapped onto the higher unit group $1+\pi^{\frac{ep}{p-1}}\mathcal{O}_K$. So to prove that f is not trés ramifié it suffices to prove that for all choices of uniformiser π of K we have that $N_{M/K}(M^\times) \not\supseteq 1+\pi^{\frac{ep}{p-1}}\mathcal{O}_K$, where $M := K(\pi^{1/p})$.

To prove this we will use the explicit description of the norm given in Serre's Local Fields [Ser79, Ch. V]. Since $M := K(\pi^{1/p})$ (for some choice of uniformiser π of K) is a totally ramified Galois extension of K of prime order p (as K contains ζ_p), the conditions are satisfied to apply the propositions of [Ser79, Ch. V, §3] to this extension. Let $\alpha := \pi^{1/p}$. Following Serre's notation, we let $t := v_M(\sigma(\alpha)-\alpha)-1$ for any generator σ of $\mathrm{Gal}(M/K)$. Taking σ to be the generator which sends $\alpha \mapsto \alpha\zeta_p$, we obtain

$$t = v_M(\alpha\cdot\zeta_p - \alpha) - 1 = v_M(\zeta_p - 1) + 1 - 1 = \frac{pe}{p-1}.$$

Letting $U_K^i := 1+\pi^i\mathcal{O}_K$ denote the higher unit groups (and similarly for M), Corollary 7 to Proposition 5 of [Ser79, Ch. V,§3] then says that, since the residue field is perfect, the canonical morphisms induced by the inclusions

$$U_K^t/N_{M/K}(U_M^t) \longrightarrow \mathcal{O}_K^\times/N_{M/K}(O_M^\times) \longrightarrow K^\times/N_{M/K}(M^\times)$$

are, in fact, isomorphisms. Note that this proposition is true specifically for the value t as defined above and fails for other higher unit groups. In other words, the natural map

$$U_K^{\frac{ep}{p-1}} \twoheadrightarrow U_K^{\frac{ep}{p-1}}/N_{M/K}(U_M^{\frac{ep}{p-1}}) \xrightarrow{\sim} K^\times/N_{M/K}(M^\times)$$

is non-zero. Note also that the group $K^\times/N_{M/K}(M^\times)$ is non-zero, for example, since it is isomorphic by local class field theory to $\mathrm{Gal}(M/K)$ which has order p. We have proved that the map $1+\pi^{\frac{ep}{p-1}}\mathcal{O}_K \to K^\times/N_{M/K}(M^\times)$ induced by inclusion is non-zero, therefore $1+\pi^{\frac{ep}{p-1}}\mathcal{O}_K \nsubseteq N_{M/K}(M^\times)$ as required. Since M was arbitrary for a choice of uniformiser π of K, this finishes the proof. $\square$

Since we already noted above that it follows from the proof of Theorem 5.4.1 [GLS15, p. 34] that $L_{V_{\underline{0},\underline{0}}}(\chi,\mathbf{1})$ equals the image of $H^1_f(G_K,\mathcal{O}_E(\tilde{\chi}_p))$ in $H^1(G_K,k_E(\chi))$, we have thus proved $L_{V_{\underline{0},\underline{0}}}(\chi,\mathbf{1}) \subseteq H^1_{\mathrm{pr}}(G_K,k_E(\chi))$ and we are done since both spaces have the same dimension.

4.3. The general Serre weight case

In this section we would like to prove Proposition 4.1.3. That is, suppose we have any two characters $\chi_1,\chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$ such that the quotient of the characters $\chi := \chi_2^{-1}\chi_1$ is the mod p cyclotomic character, and a Serre weight $V_{\underline{a},\underline{b}}$ such that $a_i - b_i + 1 < p$ for at least one i if χ_2 is unramified. Then we have that

$$L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2) \subset L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1}).$$

By the argument from before, it suffices to prove the cases

$$L_{V_{\underline{a},\underline{0}}}(\chi_1, \chi_2) \subset L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1}).$$

In the proof of this proposition we will make heavy use of the main structure theorem from Gee–Liu–Savitt [GLS15], which is stated carefully in Theorem 6.1.2. For completeness let us briefly recall the main ideas; for the details, please see §6.1. For the structure theorem we fix a Serre weight $V_{\underline{a},\underline{0}}$ or, equivalently, a set of integers $\{r_i := a_i + 1\}$ such that $r_i \in [1, p]$. We also fix two characters $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$ with quotient χ. We suppose, as before, that if χ is cyclotomic and $r_i = p$ for all i then χ_2 is ramified. Then we define the integers t_i for $i = 0, \ldots, f-1$ satisfying $t_i \in [0, e-1] \cup [r_i, r_i + e - 1]$ and $\chi_2|_{I_K} = \prod_i \omega_i^{t_i}$ and which are in some sense the smallest possible integers satisfying these two conditions (see §6.1 for a careful statement). Moreover, we define $s_i := r_i + e - 1 - t_i$. (The integers $\{t_i, s_i\}$ now correspond to the maximal and minimal rank-one Kisin modules of [GLS15, §5.3].) The main structure theorem then says that the subspace $L_{V_{\underline{a},\underline{0}}}(\chi_1, \chi_2)$ of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ consists of classes whose restriction to $H^1(G_{K_\infty}, \overline{\mathbf{F}}_p(\chi))$ can be represented by étale φ-modules $\mathcal{M}$ for which we can choose bases such that $\varphi : \mathcal{M}_{i-1} \to \mathcal{M}_i$ has the form

$$\begin{pmatrix} \varphi(e_{i-1}) & \varphi(f_{i-1}) \end{pmatrix} = \begin{pmatrix} e_i & f_i \end{pmatrix} \cdot \begin{pmatrix} u^{t_i} & y_i \\ 0 & (c)_i u^{s_i} \end{pmatrix}, \tag{4.3.1}$$

where $y_i \in \overline{\mathbf{F}}_p[\![u]\!]$ is a polynomial of which the degrees of the non-zero terms lie in the interval $[0, s_i - 1]$ if $t_i \geqslant r_i$ and $\{t_i\} \cup [r_i, s_i - 1]$ if $t_i < r_i$ and, furthermore, we allow one specific degree larger than $s_j - 1$ for any single choice of j if χ is trivial (see §6.1 for a precise formula). Here we understand $(c)_i$ to mean the following: $(c)_i = c$ if $i \equiv 0 \bmod f$ and $(c)_i = 1$ otherwise.

Note that when considering the étale φ-modules corresponding to extensions in $L_{V_{\underline{0},\underline{0}}}(\chi, \mathbf{1})$, where χ is mod p cyclotomic, the integers corresponding to the minimal and maximal Kisin modules are $s_i = e$ for all i and $t_i = 0$ for all i. Moreover, the restrictions on the degrees of the non-zero terms of the polynomials $y_i \in \overline{\mathbf{F}}_p[u]$ is simply given by $\deg(y_i) < e$ for all i except if χ is also trivial in which case we also allow for a non-zero term in degree $e + \frac{e}{p-1}$ for any single choice of i. Then translating our question about the inclusion of subspaces of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ to a question about étale φ-modules we see that we have to prove the following proposition.

PROPOSITION 4.3.1. *Suppose $V_{\underline{a},\underline{0}}$ is a Serre weight and suppose χ_1, χ_2 is a pair of characters $G_K \to k_E^\times$ such that the quotient $\chi := \chi_2^{-1}\chi_1$ is the mod p cyclotomic character. Suppose, moreover, that we are in the non-exceptional case, that is, we assume that if χ_2 is unramified then $r_i := a_i + 1 < p$ for at least one i. Let $\mathcal{M}$ be an étale φ-module corresponding an extension in $L_{V_{\underline{a},\underline{0}}}(\chi_1, \chi_2) \subset H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ after restriction to G_{K_∞}. Then, possibly after tensoring by a character, there exist choices of bases e_i, f_i of $\mathcal{M}_i$ for all $i = 0, \ldots, f-1$ such that $\varphi : \mathcal{M}_{i-1} \to \mathcal{M}_i$ is of the form*

$$\begin{pmatrix} \varphi(e_{i-1}) & \varphi(f_{i-1}) \end{pmatrix} = \begin{pmatrix} e_i & f_i \end{pmatrix} \cdot \begin{pmatrix} 1 & y_i \\ 0 & (c)_i u^e \end{pmatrix},$$

with $y_i \in \overline{\mathbf{F}}_p[u]$ a polynomial of degree $\deg(y_i) < e$ for all i except if χ is also trivial, in which case we also allow for non-zero coefficients in degree $e + \frac{e}{p-1}$. (Recall that $c \in \overline{\mathbf{F}}_p^\times$ was defined in §4.1.)

As remarked in §6.1 in non-exceptional cases the map

$$H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \xrightarrow{\text{res}} H^1(G_{K_\infty}, \overline{\mathbf{F}}_p(\chi))$$

is injective when restricted to the subspace $L_{V_{\underline{a},\underline{b}}}(\chi_1, \chi_2)$. Therefore, Proposition 4.1.3 follows directly from the corresponding étale φ-module result above.

PROOF. Let $\mathcal{M}$ be an étale φ-module as in Equation (4.3.1) coming from a class of $L_{V_{\underline{a},\underline{0}}}(\chi_1, \chi_2)$. It corresponds to an extension of characters whose restriction to inertia is given by

$$\begin{pmatrix} \prod_i \omega_i^{s_i} & * \\ 0 & \prod_i \omega_i^{t_i} \end{pmatrix}.$$

The condition that $\chi = \chi_2^{-1}\chi_1$ is mod p cyclotomic, now translates into congruence relations on $s_i - t_i$ for all i. We will treat the case in which χ is not trivial first.

Suppose that $s_i - t_i = e$ for all i. This is certainly sufficient for $\prod_i \omega_i^{s_i - t_i}$ to be mod p cyclotomic on inertia, but it is far from being necessary. Then it follows from the identity $s_i = (r_i + e - 1) - t_i$ that $t_i < r_i$ and, hence, that y_i has no terms of degree lower than t_i. In this case we can write the matrix $\varphi : \mathcal{M}_{i-1} \to \mathcal{M}_i$ as

$$u^{t_i} \otimes \begin{pmatrix} 1 & y_i u^{-t_i} \\ 0 & (c)_i u^e \end{pmatrix}$$

and $y_i u^{-t_i} \in k_E[u]$ is a polynomial of degree smaller than $s_i - t_i = e$.

Let us now study the condition that $\chi := \chi_2^{-1}\chi_1$ is the mod p cyclotomic character more carefully. The quotient satisfies $\chi_1\chi_2^{-1}|_{I_K} = \prod_i \omega_i^{s_i - t_i}$, so by the cyclotomic assumption $\prod_i \omega_i^{s_i-t_i} = \prod_i \omega_i^e$. For $i = 0, \dots, f-2$ we define $v_i := (0, \dots, 1, -p, \dots, 0)$ with the 1 in the i-th position and let $v_{f-1} := (-p, 0, \dots, 1)$. Then the equality of the two characters is equivalent to

$$(s_0 - t_0, s_1 - t_1, \dots, s_{f-1} - t_{f-1}) = (e, e, \dots, e) + \sum_{i=0}^{f-1} \alpha_i v_i$$

for coordinates $\alpha_i \in \mathbf{Z}$. Moreover, the assumption that $r_i \in [1, p]$ and $t_i, s_i \in [0, e-1] \cup [r_i, r_i + e - 1]$ together with the identity $s_i = (r_i + e - 1) - t_i$ give that $s_i - t_i \leqslant e + p - 1 - 2t_i \leqslant e + p - 1$ for all i. It follows that if α_0, say, is the smallest coefficient, then $\alpha_0 \geqslant -1$. Moreover, one negative coefficient, implies that all coefficients must be negative. But the case that $\alpha_i = -1$ for all i means that $s_i - t_i = e + p - 1$ for all i. This is excluded by the condition that if $r_i = p$ for all i then $t_i > 0$ for at least one i. Hence, in fact, $\alpha_i \in \mathbf{Z}_{\geqslant 0}$ for all i.

Therefore, suppose $\alpha_i = n_i \geqslant 0$ for all i. Then $s_i - t_i = e + n_i - n_{i-1}p$. Rewriting this gives $r_i - n_i - 1 + n_{i-1}p = 2t_i$. If $t_i \geqslant r_i$, then we see that $n_{i-1}p - t_i = t_i - r_i + n_i + 1 > 0$. Otherwise, we find that $t_i < r_i$ and hence that y_i has no non-zero terms of degree lower than t_i. Now we can twist the matrices of $\varphi : \mathcal{M}_{i-1} \to \mathcal{M}_i$ by u^{-t_i} so that they are of the form

$$\begin{pmatrix} 1 & y_i u^{-t_i} \\ 0 & (c)_i u^{e + n_i - n_{i-1}p} \end{pmatrix}.$$

The simultaneous change of bases $e_i' = e_i$, $f_i' = u^{n_i} f_i$ induces the transformation

$$\begin{pmatrix} 1 & 0 \\ 0 & u^{-n_i} \end{pmatrix} \begin{pmatrix} 1 & y_i u^{-t_i} \\ 0 & (c)_i u^{e + n_i - n_{i-1}p} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & u^{n_{i-1}p} \end{pmatrix} = \begin{pmatrix} 1 & y_i u^{pn_{i-1} - t_i} \\ 0 & (c)_i u^e \end{pmatrix}.$$

It follows from the calculation above that $y_i u^{pn_{i-1} - t_i}$ is still a polynomial. By Proposition 5.1.3 in [GLS15, p. 27] there always exists a further change of basis to ensure that the top right hand corner in all matrices has degree $< e$, thereby proving our claim for this case.

The case that χ is also trivial now follows from the above and Proposition 5.1.3 of [GLS15, p. 27], simply taking into account that the y_i have the possibility of having non-zero terms in one further degree. It is a straightforward check that this further non-zero degree becomes $e + \frac{e}{p-1}$ after our changes to get the matrices in the right form. □

4.4. Redefining the peu ramifié space

We still suppose χ is cyclotomic. We already saw that any class f in $H^1_{\mathrm{pr}}(G_K, \overline{\mathbf{F}}_p(\chi))$ arises as G_K acting on $\Gamma(\overline{K})$ for a finite flat group scheme Γ over $\mathcal{O}_K$ killed by p. As noted before, it follows from a theorem of Fontaine [Fon85, Thm. A] that the restriction of f to $G_K^{\frac{ep}{p-1}}$ is trivial. So we know that

$$H^1_{\mathrm{pr}}(G_K, \overline{\mathbf{F}}_p(\chi)) \subseteq \ker(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \to H^1(G_K^{\frac{ep}{p-1}}, \overline{\mathbf{F}}_p(\chi))).$$

In §5.1 this kernel is denoted by $\mathrm{Fil}^{<1+\frac{ep}{p-1}} H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. By Dembélé-Diamond-Roberts [DDR16] this kernel is referred to as the 'typically ramified subspace'. However, it follows from Proposition 5.1.3 that the subspace $\mathrm{Fil}^{<1+\frac{ep}{p-1}} H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ has codimension 1 in $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. Therefore, we have an equality of these two spaces and we can give the following equivalent redefinition of the peu ramifié space.

Corollary 4.4.1. *Suppose χ is cyclotomic. The* ***peu ramifié subspace*** *of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ is given by*

$$\begin{aligned} H^1_{\mathrm{pr}}(G_K, \overline{\mathbf{F}}_p(\chi)) &= \ker\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \to H^1(G_K^{\frac{ep}{p-1}}, \overline{\mathbf{F}}_p(\chi))\right) \\ &= \left\{ f \in H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \;\middle|\; f|_{G_K^{\frac{ep}{p-1}}} = \mathbf{1} \right\}. \end{aligned}$$

CHAPTER 5

Explicit bases of spaces of extensions

In this chapter we define an explicit basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ in terms of local class field theory and the Artin–Hasse exponential. In the next chapter we will use this basis to give an explicit description of the distinguished subspaces L_V from §3.3. Let us emphasise that the basis elements in this chapter may depend on the choice of uniformiser we make, but in the next chapter we will take an appropriate subset of basis elements spanning a subspace which is independent of this choice.

To anyone familiar with the paper of Dembélé, Diamond and Roberts [DDR16] it will be clear that this chapter owes a great deal to their ideas. In particular, §5.1, §5.2 and §5.3 are direct generalisations of §3 and §5 of [DDR16] to the case where K is an arbitrary extension of $\mathbf{Q}_p$ – they assume K is unramified over $\mathbf{Q}_p$. The presentation and a number of the arguments are directly analogous to the presentation and arguments given in [DDR16]; we will not continue to mention this throughout the chapter. We invite the curious reader to have a look at [DDR16] for a comparison.

5.1. The filtration on $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$

Let π be a root of $x^{p^f-1} + \pi_K$ in $\overline{K}$. Recall that we have a character $\overline{\omega}_\pi : G_K \to k^\times$ defined by $\sigma \mapsto \sigma(\pi)/\pi$. For $i = 0, \dots, f-1$, we get the fundamental characters $\omega_i : G_K \to \overline{\mathbf{F}}_p^\times$ of level f by $\omega_i := \overline{\tau}_i \circ \overline{\omega}_\pi$. If $\chi : G_K \to \overline{\mathbf{F}}_p^\times$ is any continuous character, then we can write $\chi|_{I_K} = \prod_i \omega_i^{a_i}|_{I_K}$ for $a_i \in [1, p]$.[1] The f-tuple $(a_0, a_1, \dots, a_{f-1})$ is uniquely determined by $\chi|_{I_K}$ if we, furthermore, require that $a_i < p$ for at least one i. We will call this f-tuple the **tame signature** of χ; this is an element of the set

$$S := \{1, 2, \dots, p\}^f - \{(p, p, \dots, p)\}.$$

[1]Our choice of $a_i \in [1, p]$ instead of $a_i \in [0, p-1]$ is mainly to be consistent with the conventions of [DDR16]. None of the results in this chapter or the next depend on this convention, but some of the combinatorial results from Chapter 7 may change with a different convention – it is possible that easier combinatorics was the motivation of this choice in [DDR16] initially.

We define an action of $\mathrm{Gal}(k/\mathbf{F}_p) = \langle \mathrm{Frob} \rangle \cong \mathbf{Z}/f\mathbf{Z}$ on the set S via

$$\mathrm{Frob} \cdot (a_0, a_1, \ldots, a_{f-1}) = (a_1, a_2, \ldots, a_0).$$

Note that this notation makes sense since if χ has tame signature $\vec{a}$, then $\mathrm{Frob} \circ \chi$ has tame signature $\mathrm{Frob}(\vec{a})$. We define the **period** of $\vec{a} \in S$ to be the cardinality of its orbit in S under the action of $\mathrm{Gal}(k/\mathbf{F}_p)$. We will call the period of the tame signature of χ the **absolute niveau** of the character. We will write f' for the absolute niveau of χ and $f'' := f/f'$ for the size of the stabiliser of the action of $\mathrm{Gal}(k/\mathbf{F}_p)$. Whenever convenient we will consider the indices of the a_i to be elements of $\mathbf{Z}/f\mathbf{Z}$, so $a_f = a_0$ etcetera. We can also write $\chi|_{I_K} = \omega_i^{n_i}|_{I_K}$ for all $0 \leqslant i < f$, where we define[2]

$$n_i := \sum_{j=1}^{f} a_{i+j} p^{f-j} = a_{i+1} p^{f-1} + \cdots + a_{i+f-1} p + a_i.$$

5.1.1. Definition of the filtration. Suppose χ is a continuous character $G_K \to \overline{\mathbf{F}}_p^\times$. Recall from [Ser79, Ch. IV,§3] that we have a decreasing filtration on G_K by closed subgroups G_K^u given by the upper numbering on G_K for $u \in \mathbf{R}$. Recall also that $G_K^u = G_K$ for $u \leqslant -1$, that for $-1 < u \leqslant 0$ we have $G_K^u = I_K$, the inertia subgroup of G_K, and that $\bigcup_{u>0} G_K^u = P_K$, the wild inertia subgroup of G_K. For $s \in \mathbf{R}$, we will define an **increasing filtration** Fil^s on $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ by the rule

$$\mathrm{Fil}^s H^1(G_K, \overline{\mathbf{F}}_p(\chi)) := \bigcap_{u>s-1} \ker\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \xrightarrow{\mathrm{res}} H^1(G_K^u, \overline{\mathbf{F}}_p(\chi))\right).$$

We will, furthermore, define

$$\mathrm{Fil}^{<s} H^1(G_K, \overline{\mathbf{F}}_p(\chi)) := \bigcup_{t<s} \mathrm{Fil}^t H^1(G_K, \overline{\mathbf{F}}_p(\chi))$$

and define the associated grading by

$$\mathrm{gr}^s\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi))\right) := \frac{\mathrm{Fil}^s H^1(G_K, \overline{\mathbf{F}}_p(\chi))}{\mathrm{Fil}^{<s} H^1(G_K, \overline{\mathbf{F}}_p(\chi))}.$$

5.1.1.1. *The filtration for $s \leqslant 1$.* Let us first study this filtration on the interval $s \in (-\infty, 1]$. We see immediately that $\mathrm{Fil}^s H^1(G_K, \overline{\mathbf{F}}_p(\chi)) = 0$ for any $s < 0$. For $0 \leqslant s < 1$, we have

$$\mathrm{Fil}^s H^1(G_K, \overline{\mathbf{F}}_p(\chi)) = \ker\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \xrightarrow{\mathrm{res}} H^1(I_K, \overline{\mathbf{F}}_p(\chi))\right).$$

[2]We note that our definition of n_i differs from [DDR16], since we assumed our embeddings to satisfy $\overline{\tau}_{i+1}^p = \overline{\tau}_i$ rather than $\overline{\tau}_i^p = \overline{\tau}_{i+1}$ as is assumed there.

Since $\bigcup_{u>0} G_K^u = P_K$, a class c of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ lies in $\mathrm{Fil}^1 H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ if and only if $z(P_K) = 0$ for any cocycle z representing c. Since P_K is the maximal pro-p subgroup of I_K, we see that $H^1(I_K/P_K, \overline{\mathbf{F}}_p(\chi)) = 0$ and it follows from inflation-restriction that the restriction map

$$H^1(I_K, \overline{\mathbf{F}}_p(\chi)) \to H^1(P_K, \overline{\mathbf{F}}_p(\chi))$$

is injective. Therefore, any cocycle with trivial restriction to P_K must also have trivial restriction to I_K. In other words,

$$\mathrm{Fil}^1 H^1(G_K, \overline{\mathbf{F}}_p(\chi)) = \mathrm{Fil}^0 H^1(G_K, \overline{\mathbf{F}}_p(\chi)).$$

5.1.1.2. *Filtered piece as kernel.* Suppose that $s > 1$. If z is a cocycle representing a cohomology class in $\mathrm{Fil}^{<s}$, then clearly $z(G_K^{s-1}) = 0$. Conversely, if z is a continuous cocycle such that $z(G_K^{s-1}) = 0$, then it follows from the identity $G_K^{s-1} = \bigcap_{v<s-1} G_K^v$ that

$$\ker(z) \cup \bigcup_{v<s-1} (G_K - G_K^v)$$

is an open cover of G_K. Compactness of G_K then implies that there is a $v_0 < s-1$ such that $G_K^{v_0} \subseteq \ker(z)$. In other words, we have just proved that

$$\mathrm{Fil}^{<s} H^1(G_K, \overline{\mathbf{F}}_p(\chi)) = \ker\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \xrightarrow{\mathrm{res}} H^1(G_K^{s-1}, \overline{\mathbf{F}}_p(\chi))\right).$$

5.1.2. The jumps in the filtration. Having defined the filtration and its most basic properties, we are now interested in the jumps of the filtration and the size of these jumps. That is, we would like to study the dimensions of the spaces $\mathrm{gr}^s\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi))\right)$. Fix a continuous character $\chi : G_K \to \overline{\mathbf{F}}_p^\times$ and let the n_i for $i = 0, \ldots, f-1$ be as above. The following theorem gives the answer.

THEOREM 5.1.1. *For $s \in \mathbf{R}$, write $d_s := \dim_{\overline{\mathbf{F}}_p} \mathrm{gr}^s\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi))\right)$. Then $d_s = 0$ unless $s = 0$ or $1 < s \leqslant 1 + \frac{pe}{p-1}$. Moreover, if $1 < s < 1 + \frac{pe}{p-1}$ and $d_s \neq 0$ then $s = 1 + \frac{m}{p^f-1}$ for an integer $m \not\equiv 0 \bmod p$. More precisely, the dimensions d_s are given by*

(1) $d_0 = 1$ if χ is trivial and $d_0 = 0$ otherwise.
(2) if $1 < s < 1 + \frac{pe}{p-1}$ and $s = 1 + \frac{m}{p^f-1}$ for $p \nmid m$, then

$$d_s = \#\left\{i \in \{0, \ldots, f-1\} \mid m \equiv n_i \bmod p^f - 1\right\}.$$

(3) $d_{1+\frac{ep}{p-1}} = 1$ if χ is cyclotomic and $d_{1+\frac{ep}{p-1}} = 0$ otherwise.

REMARK 5.1.2. Note that if $t, u \in \{0, \ldots, f-1\}$ are such that n_t and n_u are both congruent to $m \bmod (p^f - 1)$ then the uniqueness of the n_i modulo $(p^f - 1)$ implies that $n_t = n_u$. Hence, either $t = u$ or $\vec{a}$ has a non-trivial stabilizer in $\mathrm{Gal}(k/\mathbf{F}_p)$. This observation implies that, for $1 < s < 1 + \frac{pe}{p-1}$, we have that $d_s = f/f'$ whenever $d_s > 0$, where f' is the absolute niveau of χ.

For the theorem to make sense, of course, the sum of the dimensions d_s must add up to the $\overline{\mathbf{F}}_p$-dimension of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. Since we will need this in the proof of the theorem, let us prove it first. To contrast the actual dimensions of the graded pieces with the dimensions claimed in the second part of the theorem above, let us write d'_s for the values of the dimensions claimed in the theorem.

Proposition 5.1.3. *For $j = 0, \ldots, e-1$, we have*

$$\sum_{\frac{jp}{p-1} < \frac{m}{p^f-1} < \frac{(j+1)p}{p-1}} d'_{1+\frac{m}{p^f-1}} = f.$$

Remark 5.1.4. In fact, the proposition and Remark 5.1.2 above imply that for any $j \geqslant 0$ the set of integers $m \in \mathbf{Z}$ satisfying

(1) $\frac{jp}{p-1} < \frac{m}{p^f-1} < \frac{(j+1)p}{p-1}$,
(2) $p \nmid m$ and
(3) there exists an i such that $m \equiv n_i \bmod (p^f - 1)$

has cardinality f', where f' is the absolute niveau of χ. We will need this later in §5.3.

Proof. We have the inequalities $\frac{1}{p-1} \leqslant \frac{n_i}{p^f-1} < \frac{p}{p-1}$ for all i. It is easy to show explicitly that there exists a unique integer k_j such that

$$\left(\left[\frac{1}{p-1}, \frac{p}{p-1}\right) + k_j\right) \cap \left(\frac{jp}{p-1}, \frac{(j+1)p}{p-1}\right) \neq \varnothing$$

and

$$\left(\left[\frac{1}{p-1}, \frac{p}{p-1}\right) + k_j + 1\right) \cap \left(\frac{jp}{p-1}, \frac{(j+1)p}{p-1}\right) \neq \varnothing.$$

Moreover, if we write $j - 1 \equiv b \bmod p-1$ for $0 \leqslant b < p-1$ (when $p = 2$ we simply let $b = 0$), then we can show $k_j \equiv b+1 \bmod p$. We are interested in counting the number of n_i that satisfy

$$\frac{jp}{p-1} < \frac{n_i}{p^f-1} + k_j \text{ and } n_i + k_j(p^f-1) \not\equiv 0 \bmod p \tag{5.1.1}$$

or

$$\frac{n_i}{p^f-1} + (k_j+1) < \frac{(j+1)p}{p-1} \text{ and } n_i + (k_j+1)(p^f-1) \not\equiv 0 \bmod p \tag{5.1.2}$$

or both, in which case they should be counted twice. We don't have to worry about upper or lower bounds in the first or second case, respectively, since these are automatically satisfied.

In the case of Equation (5.1.1) the inequality reduces to the inequality

$$\frac{n_i}{p^f - 1} > \frac{b+1}{p-1}.$$

This inequality is satisfied if and only if n_i has coordinates

$$(a_i, a_{i+1}, \dots, a_j, \dots) = (a_i, b+1, b+1, \dots, b+1, a_j, \dots)$$

with $a_j > b+1$. If we, furthermore, require that $n_i + k_j(p^f - 1) \not\equiv 0 \bmod p$, we see that this requirement is equivalent to requiring that $a_i \neq b+1$. Hence, the number of such n_i is the same as the number $\#\{a_j > b+1\}$.

In the case of Equation (5.1.2) the inequality reduces to the inequality

$$\frac{n_i}{p^f - 1} < \frac{b+2}{p-1}.$$

This inequality is satisfied if and only if n_i corresponds to a tuple

$$(a_i, a_{i+1}, \dots, a_j, \dots) = (a_i, b+2, b+2, \dots, b+2, a_j, \dots)$$

with $a_j \leqslant b+1$. If we also require $n_i + (k_j + 1)(p^f - 1) \not\equiv 0 \bmod p$, we find that $a_i \neq b+2$. Hence, in this case we see that the number of n_i satisfying both conditions is $\#\{a_j \leqslant b+1\}$.

It follows that the total number of n_i satisfying one of these equations, counted with multiplicity, is

$$\#\{a_j > b+1\} + \#\{a_j \leqslant b+1\} = f.$$

$\square$

A straightforward calculation using the local Euler-Poincaré characteristic gives

$$\dim_{\overline{\mathbf{F}}_p} H^1(G_K, \overline{\mathbf{F}}_p(\chi)) = \begin{cases} ef + 2 & \text{if } \chi \text{ is both trivial and cyclotomic;} \\ ef + 1 & \text{if } \chi \text{ is trivial, but not cyclotomic;} \\ ef + 1 & \text{if } \chi \text{ is cyclotomic, but not trivial;} \\ ef & \text{otherwise.} \end{cases}$$

From the proposition above and this observation we immediately get the following corollary.

COROLLARY 5.1.5. *Let the d'_s denote the dimensions as claimed in Theorem 5.1.1. Then*

$$\sum_{1<s<1+\frac{ep}{p-1}} d'_s = ef.$$

Hence, we find $\sum_s d'_s = \dim_{\overline{\mathbf{F}}_p} H^1(G_K, \overline{\mathbf{F}}_p(\chi))$.

PROOF OF THEOREM 5.1.1. Let us write d'_s again for the values of d_s claimed in the second part of Theorem 5.1.1. By Corollary 5.1.5 we know that $\sum_s d'_s = \sum_s d_s$, hence it suffices to consider only $s \in \mathbf{R}$ such that $d'_s > 0$ and prove $d'_s = d_s$ for these values of s.

Let us first treat the case $s = 0$. We already saw above that

$$\mathrm{Fil}^0 H^1(G_K, \overline{\mathbf{F}}_p(\chi)) = \ker\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \xrightarrow{\text{res}} H^1(I_K, \overline{\mathbf{F}}_p(\chi))\right)$$

and $\mathrm{Fil}^s = 0$ for $s < 0$. We can use the inflation-restriction exact sequence to show that the kernel above is isomorphic to $H^1\left(G_K/I_K, \overline{\mathbf{F}}_p(\chi)^{I_K}\right)$. This space is clearly 1-dimensional over $\overline{\mathbf{F}}_p$ if χ is trivial and 0-dimensional if χ is ramified. However, if χ is unramified and non-trivial, by identifying G_K/I_K with $\hat{\mathbf{Z}}$, we may consider χ as a character $\hat{\mathbf{Z}} \to \overline{\mathbf{F}}_p^\times$. By continuity any representation of $\hat{\mathbf{Z}}$ is completely determined by the image of 1. An extension of $\overline{\mathbf{F}}_p$ by $\overline{\mathbf{F}}_p(\chi)$ is always split since the matrix corresponding to 1 has distinct eigenvalues over an algebraically closed field (as χ is non-trivial). Hence, $\dim_{\overline{\mathbf{F}}_p} H^1\left(G_K/I_K, \overline{\mathbf{F}}_p(\chi)^{I_K}\right) = 1$ if χ is trivial and 0 otherwise.

Assume that $1 < s \leqslant 1 + \frac{ep}{p-1}$ and $m := (s-1)(p^f - 1)$. We define an extension M/K by letting $M := L(\pi)$ for π a root of $x^{p^f-1} + \pi_K$ and L/K an unramified extension of degree prime to p such that $\chi|_{G_M}$ is trivial. The extension M is now a tamely ramified Galois extension of K of ramification degree $p^f - 1$ and $\mathrm{Gal}(M/K)$ has order prime to p. Combined with the inflation-restriction sequence

$$0 \to H^1(\mathrm{Gal}(M/K), \overline{\mathbf{F}}_p(\chi)) \to H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \to H^1(G_M, \overline{\mathbf{F}}_p(\chi))^{\mathrm{Gal}(M/K)}$$

this gives

$$H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \cong H^1(G_M, \overline{\mathbf{F}}_p(\chi))^{\mathrm{Gal}(M/K)} = \mathrm{Hom}_{\mathrm{Gal}(M/K)}(G_M^{\mathrm{ab}}, \overline{\mathbf{F}}_p(\chi)).$$

The isomorphisms of local class field theory give an isomorphism

$$G_M^{\mathrm{ab}} \otimes \mathbf{F}_p \cong M^\times/(M^\times)^p,$$

and we obtain

$$H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \cong \mathrm{Hom}_{\mathrm{Gal}(M/K)}(M^\times/(M^\times)^p, \overline{\mathbf{F}}_p(\chi)).$$

Since M/K is tamely ramified of ramification degree $p^f - 1$, we know that Hasse-Herbrand function is given by $\psi_{M/K}(x) = (p^f - 1)x$ for $x \geqslant 0$ and that $G_K^u \subset G_M$ for any $u > 0$. Using Proposition IV.15 [Ser79, p. 74], it follows that for any finite extension M'/M and any $u > 0$ we have

$$\mathrm{Gal}(M'/K)^u = \mathrm{Gal}(M'/M)_{\psi_{M'/M}((p^f-1)u)} = \mathrm{Gal}(M'/M)^{(p^f-1)u}.$$

So $G_K^u = G_M^{(p^f-1)u}$ for $u > 0$. Moreover, the maps of local class field theory map $G_M^{(p^f-1)u}$ onto the unit group $1 + \pi^{\lceil (p^f-1)u \rceil}\mathcal{O}_M$ by Corollary 3 to Theorem XV.1 in [Ser79, p. 228]. If we denote the unit group $1 + \pi^i\mathcal{O}_M$ by U_i for any integer $i > 0$, then it becomes apparent that a cocycle in $c \in H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ has trivial restriction to G_K^u for all $u > s-1$ (to G_K^{s-1}, resp.) if and only if the corresponding homomorphism $M^\times/(M^\times)^p \to \overline{\mathbf{F}}_p(\chi)$ factors through $M^\times/(M^\times)^p U_{m+1}$ (through $M^\times/(M^\times)^p U_m$, resp.), where we still let $m = (s-1)(p^f-1)$. Note that this is precisely the condition such that $c \in \mathrm{Fil}^s H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ ($c \in \mathrm{Fil}^{<s} H^1(G_K, \overline{\mathbf{F}}_p(\chi))$, resp.) and it follows that

$$\mathrm{gr}^s\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi))\right) \cong \mathrm{Hom}_{\mathrm{Gal}(M/K)}\left(\frac{U_m}{(U_m \cap (M^\times)^p)U_{m+1}}, \overline{\mathbf{F}}_p(\chi)\right).$$

First assume $1 < s < 1 + \frac{ep}{p-1}$ and $p \nmid m := (s-1)(p^f-1)$. This is equivalent to the requirement that $0 < m < \frac{ep(p^f-1)}{(p-1)}$. We claim that $U_m \cap (M^\times)^p \subset U_{m+1}$. Let $x = 1 + u\pi^t$ for positive integer t and a unit $u \in \mathcal{O}_M^\times$ and suppose $v_M(x^p - 1) \geqslant m$. But

$$v_M(x^p - 1) = v_M(pu\pi^t + \cdots + u^p\pi^{pt}) \geqslant \min(e(p^f-1)+t, pt)$$

with equality unless $e(p^f-1)+t = pt$. If $pt < e(p^f-1)+t$, then $m = pt$, which would contradict the condition $p \nmid m$. On the other hand, if $e(p^f-1)+t \leqslant pt$, then $t \geqslant \frac{e(p^f-1)}{p-1}$ gives $e(p^f-1)+t \geqslant \frac{ep(p^f-1)}{(p-1)}$ and, therefore, $m = e(p^f-1)+t$ would contradict the upper bound on m. Hence, $v_M(x^p-1) \geqslant m+1$ as required. It follows from the claim that

$$\mathrm{gr}^s\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi))\right) \cong \mathrm{Hom}_{\mathrm{Gal}(M/K)}\left(U_m/U_{m+1}, \overline{\mathbf{F}}_p(\chi)\right).$$

We let l denote the residue field of L. The action of $\sigma \in \mathrm{Gal}(M/K)$ on U_m/U_{m+1} sends $1 + x\pi^m \mapsto 1 + \sigma(x)\overline{\omega}_\pi(\sigma)\pi^m$. Therefore, we have a $\mathrm{Gal}(M/K)$-equivariant isomorphism

$$l(\overline{\omega}_\pi^m) \xrightarrow[x \mapsto 1+x\pi^m]{} U_m/U_{m+1}.$$

Let S_i be the set of embeddings $l \to \overline{\mathbf{F}}_p$ which restrict to $\overline{\tau}_i$ over k. Then the map

$$\begin{aligned} l(\overline{\omega}_\pi^m) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p &\cong \bigoplus_{i=0}^{f-1} \left(\bigoplus_{\tau \in S_i} \overline{\mathbf{F}}_p(\omega_i^m) \right) \\ x \otimes 1 &\mapsto (\tau(x))_\tau \end{aligned}$$

is a $\mathrm{Gal}(M/K)$-equivariant isomorphism, where the action of $\mathrm{Gal}(M/K)$ on $\bigoplus_{\tau \in S_i} \overline{\mathbf{F}}_p(\omega_i^m)$ is defined by $g \cdot ((x_\tau)_\tau) = (\omega_i^m(g) x_{\tau \circ g})_\tau$. (This is the well-known isomorphism

$$\begin{aligned} l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p &\cong \bigoplus_{\tau : l \hookrightarrow \overline{\mathbf{F}}_p} \overline{\mathbf{F}}_p; \\ x \otimes 1 &\mapsto (\tau(x))_\tau, \end{aligned}$$

in which we keep track of the Galois action.) We note that

$$\bigoplus_{\tau \in S_i} \overline{\mathbf{F}}_p \cong \mathrm{Ind}_{\mathrm{Gal}(M/L)}^{\mathrm{Gal}(M/K)} \overline{\mathbf{F}}_p.$$

The latter representation is just the regular representation of the quotient $\mathrm{Gal}(L/K)$. Since this group is finite abelian of order prime-to-p, its regular representation decomposes as a direct sum of all its 1-dimensional representations, i.e.

$$\mathrm{Ind}_{\mathrm{Gal}(M/L)}^{\mathrm{Gal}(M/K)} \overline{\mathbf{F}}_p \cong \bigoplus_{\nu : \mathrm{Gal}(L/K) \to \overline{\mathbf{F}}_p^\times} \overline{\mathbf{F}}_p(\nu),$$

and hence we find that

$$l(\overline{\omega}_\pi^m) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p \cong \bigoplus_{i=0}^{f-1} \left(\bigoplus_{\nu} \overline{\mathbf{F}}_p(\nu \omega_i^m) \right).$$

It follows that the dimension of $\mathrm{gr}^s \left(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \right)$ is equal to

$$\dim_{\overline{\mathbf{F}}_p} \mathrm{Hom}_{\mathrm{Gal}(M/K)} \left(\bigoplus_{i=0}^{f-1} \left(\bigoplus_{\nu} \overline{\mathbf{F}}_p(\nu \omega_i^m) \right), \overline{\mathbf{F}}_p(\chi) \right)$$

and this dimension is equal to the number of i such that $m \equiv n_i \bmod p^f - 1$, which proves that $d'_s = d_s$ for all $1 < s < 1 + \frac{ep}{p-1}$ for which $d'_s > 0$.

Finally, assume $s = 1 + \frac{ep}{p-1}$, or, equivalently, assume $m = \frac{ep(p^f-1)}{p-1}$. We may, furthermore, assume that χ is cyclotomic, since we are only considering cases in which $d'_s > 0$. Note that the requirement that $\chi|_{G_M}$ is trivial implies that $\zeta_p \in M$. To show $d_s = d'_s = 1$, by the earlier calculation, is equivalent to showing

$$\mathrm{Hom}_{\mathrm{Gal}(M/K)} \left(\frac{U_m}{(U_m \cap (M^\times)^p) U_{m+1}}, \overline{\mathbf{F}}_p(\chi) \right)$$

is 1-dimensional. We will prove that the quotient of unit groups is isomorphic to $\mathbf{F}_p(\chi)$ as an $\mathbf{F}_p[\mathrm{Gal}(M/K)]$-module from which the required result is immediate. Similarly to the calculation on valuations above, it is easy to show $U_m \cap (M^\times)^p = (U_n)^p$ where $n = m/p$. We can obtain the quotient $U_m/(U_m \cap (M^\times)^p)U_{m+1}$, therefore, as the cokernel of the p-power map

$$U_n/U_{n+1} \xrightarrow[x \longmapsto x^p]{} U_m/U_{m+1}.$$

A small calculation shows that this map sends $1 + s\pi^n \mapsto 1 + (s^p + cs)\pi^m$, where $c \in \mathcal{O}_M^\times$ is defined by $p = c\pi^{e(p^f-1)}$. Since $\zeta_p \in M$, we know that M contains $N := \mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p(\sqrt[p-1]{-p})$. Therefore, there exists a unit $u \in \mathcal{O}_M^\times$ such that $\pi^{e(p^f-1)} = (u \sqrt[p-1]{-p})^{p-1} = -u^{p-1}p$ giving $-c = (u^{-1})^{p-1}$. We conclude that $-c$ always has a $(p-1)$st root in the residue field and that the p-power map above has kernel and, thus, cokernel of size p. Write $\overline{s}$ for the image of any $s \in \mathcal{O}_M^\times$ in the cokernel. The action of $\mathrm{Gal}(M/K)$ on this cokernel is given by $\overline{\omega}_\pi^m \otimes \mu_{-\overline{c}}$ where $\mu_\alpha : \mathrm{Gal}(M/K) \to \mathbf{F}_p^\times$ is the unramified character sending the (absolute) arithmetic Frobenius Frob_p to $\alpha \in \mathbf{F}_p^\times$. For any uniformiser π_N of N, we can write $\zeta_p = v\pi_N + 1$ for a unit $v \in \mathcal{O}_N^\times$. Hence, one sees that for $\sigma \in \mathrm{Gal}(M/K)$ we have

$$\frac{\sigma(v\pi_N)}{v\pi_N} = \frac{(1 + v\pi_N)^{\chi(\sigma)} - 1}{v\pi_N} \equiv \chi(\sigma) \bmod \pi.$$

Since $\sigma(v)/v \equiv 1 \bmod \pi$, it follows that $\sigma(\pi_N)/\pi_N \equiv \chi(\sigma) \bmod \pi$ for any uniformiser π_N of N, in particular $\pi_N = \sqrt[p-1]{-p}$. Thence, if $\sigma \in \mathrm{Gal}(M/K)$ is a lift of Frob_p, then

$$\overline{\omega}_\pi(\sigma)^n = \frac{\sigma(u \sqrt[p-1]{-p})}{u \sqrt[p-1]{-p}} \equiv \overline{u}^{p-1}\chi(\sigma) = (-\overline{c})^{-1}\chi(\sigma).$$

In other words, we've just shown that $\overline{\omega}_\pi^n$ acts as $\chi \otimes \mu_{-\overline{c}^{-1}}$ on the cokernel and, therefore, $\overline{\omega}_\pi^m$ must act on the cokernel in the same way since $(p^f - 1) \mid m - n$. Thus, $\mathrm{Gal}(M/K)$ acts on the cokernel via the cyclotomic character and $U_m/(U_m \cap (M^\times)^p)U_{m+1} \cong \mathbf{F}_p(\chi)$, as required. $\square$

5.2. Constructing the basis elements

In this section we will construct explicit basis elements of the space $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$, which we will later use to give an explicit version of Serre's conjecture. We will construct the basis by making certain choices and only at the end of the next chapter it will follow that our construction is independent of the choices made.

5.2.1. The Artin-Hasse Exponential. Before we move on to define a basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ explicitly, we must first define a homomorphism ε_α in terms of which our basis will be defined. Recall that the **Artin-Hasse exponential** is given by

$$E_p(x) = \exp\left(\sum_{n\geqslant 0} \frac{x^{p^n}}{p^n}\right).$$

It's a well-known fact that $E_p(x)$ is an element of $\mathbf{Z}_p[\![x]\!]$ (see, for example, [Rob00, §7.2.2]), i.e. its coefficients are p-integral elements of $\mathbf{Q}$. Since p is fixed throughout, we will write $E(x)$ instead of $E_p(x)$ from now on.

Suppose l is a finite field of characteristic p and L is the field of fractions of the ring of Witt vectors $W(l)$ of l. Let M be a subfield of $\mathbf{C}_p$ containing L and let $\alpha \in M$ be such that $|\alpha| < 1$. We define a map

$$\begin{aligned} \varepsilon_\alpha : l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p &\to \mathcal{O}_M^\times \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p \\ a \otimes b &\mapsto E([a]\alpha) \otimes b, \end{aligned} \tag{5.2.1}$$

where $[a]$ is a Teichmüller lift of $a \in l$. It follows from [DDR16, Lem. 4.1] that this map is a homomorphism which relates the additive structure of l to the multiplicative structure of $\mathcal{O}_M^\times \otimes \mathbf{F}_p$. We will use this homomorphism to construct an explicit basis for $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$.

5.2.2. An $\overline{\mathbf{F}}_p$-dual of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. We need a slightly more general set-up than in the previous section. Suppose $K/\mathbf{Q}_p$ is a finite extension of ramification index e, of residue degree f and with residue field k. Moreover, we take $\chi : G_K \to \overline{\mathbf{F}}_p^\times$ to be any continuous character. Let $M = L(\pi)$ be a totally tamely ramified extension of an unramified prime-to-p-degree extension L/K, where the ramification degree e_M of M/K satisfies $e_M \mid p^f - 1$ and the uniformiser π of M satisfies $\pi^{e_M} \in K^\times$, and we take M sufficiently large so that $\chi|_{G_M}$ is trivial. Note that e_M denotes the ramification degree of M over K, and the ramification degree $e_{M/\mathbf{Q}_p}$ of M over $\mathbf{Q}_p$ is given by $e_{M/\mathbf{Q}_p} = e_M e$. We recover the set-up of the previous section by taking $e_M = p^f - 1$ and $\pi^{e_M} = -\pi_K$. Note that the proof of Theorem 5.1.1 follows in the same way as before, taking into account that now $s = 1 + \frac{m}{e_M}$. In particular, for $1 < s \leqslant 1 + \frac{ep}{p-1}$ we still have the isomorphism

$$\mathrm{gr}^s\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi))\right) \cong \mathrm{Hom}_{\mathrm{Gal}(M/K)}\left(\frac{U_m}{(U_m \cap (M^\times)^p)U_{m+1}}, \overline{\mathbf{F}}_p(\chi)\right),$$

which, if we furthermore require that $s < 1 + \frac{ep}{p-1}$ and $p \nmid m := e_M(s-1)$, can again be shown to simplify to

$$\mathrm{gr}^s\left(H^1(G_K, \overline{\mathbf{F}}_p(\chi))\right) \cong \mathrm{Hom}_{\mathrm{Gal}(M/K)}\left(U_m/U_{m+1}, \overline{\mathbf{F}}_p(\chi)\right).$$

More generally, for this choice of M we certainly still have

$$\begin{aligned} H^1(G_K, \overline{\mathbf{F}}_p(\chi)) &\cong \mathrm{Hom}_{\mathrm{Gal}(M/K)}\left(M^\times, \overline{\mathbf{F}}_p(\chi)\right) \\ &\cong \mathrm{Hom}_{\overline{\mathbf{F}}_p}\left(\left(M^\times \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M/K)}, \overline{\mathbf{F}}_p\right). \end{aligned}$$

We will construct our basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ as a dual basis to a basis for the space above, therefore it will be useful to give this space a name. Let

$$U_\chi := \left(M^\times \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M/K)}.$$

5.2.3. The basis elements $u_{i,j}$. Letting f' denote the absolute niveau of χ and $f'' := f/f'$, recall from Section 5.1.2 that for any $0 \leqslant j < e$ the set of integers $m \in \mathbf{Z}$ satisfying

(1) $\frac{jp}{p-1} < \frac{m}{p^f-1} < \frac{(j+1)p}{p-1}$,
(2) $p \nmid m$ and
(3) there exists an i such that $m \equiv n_i \bmod (p^f - 1)$

has cardinality f'. We order these integers in whichever way and denote them by $\{m_{0,j}, m_{1,j}, \dots, m_{f'-1,j}\}$. Then there must exist a unique map

$$\phi_j \colon \{0, \dots, f'-1\} \to \{0, \dots, f'-1\}$$

such that $m_{i,j} \equiv n_{\phi_j(i)} \bmod (p^f - 1)$ – recall that the set of all n_i has cardinality f'. Note that the map ϕ_j may not be injective. Let us write i' from now on for subscripts in $\mathbf{Z}/f'\mathbf{Z}$ to avoid confusion with the $\mathbf{Z}/f\mathbf{Z}$-setting. In formulae involving an $i \in \mathbf{Z}/f\mathbf{Z}$ we will implicitly use $i = i' + kf'$ for $0 \leqslant i' < f'$ and $0 \leqslant k < f''$ to fix the values of i' and k; for the sake of brevity will often sometimes write $\phi_j(i)$ for $\phi_j(i') + kf'$. Trivially, we also get the congruence $m_{i',j} \equiv n_{\phi_j(i')+kf'} \bmod (p^f - 1)$.

Let us return to the situation where $M = L(\pi)$ for an unramified extension L of K of degree prime-to-p and a uniformiser π such that $\pi^{e_M} \in K^\times$ and $\chi|_{G_M}$ is trivial. This implies that $\chi|_{I_K}$ factors through $I_{M/K}$ which has cardinality e_M, so for any i we see $(\chi|_{I_K})^{e_M} = \omega_i^{n_i e_M} = \mathbf{1}$. Any n_i, therefore, is divisible by $(p^f - 1)/e_M$. It follows that the set of integers $m' \in \mathbf{Z}$ satisfying the three conditions

(1) $\frac{jp}{p-1} < \frac{m'}{e_M} < \frac{(j+1)p}{p-1}$,
(2) $p \nmid m'$ and
(3) there exists an i such that $m' \equiv \frac{e_M n_i}{p^f-1} \bmod e_M$

is in bijection with the set above by the explicit map $m \mapsto m' := \frac{e_M m}{p^f-1}$. We will write ω_π for the character $G_K \to K^\times$ defined by $\sigma \mapsto \sigma(\pi)/\pi$ and $\overline{\omega}_\pi$ for its reduction mod π_K. We note that this character factors through $\mathrm{Gal}(M/K)$ and, since $\sigma(\pi)$ is a root of $x^{e_M} - \pi^{e_M} \in K[x]$, the image of ω_π is contained in $\mu_{e_M}(K)$, the e_Mth roots of unity in $K^\times$. To contrast this with our previous fundamental character, let us from now on write $\overline{\omega}_{\mathrm{fc}} : G_K \to k^\times$ for the mod p character defined by $\sigma \mapsto \sigma(\alpha)/\alpha$ for α a root of $x^{p^f-1} + \pi_K$. We have $\overline{\omega}_\pi|_{I_K} = (\overline{\omega}_{\mathrm{fc}}|_{I_K})^{(p^f-1)/e_M}$, and, therefore, for all $0 \leqslant i < f$, we have

$$\chi|_{I_K} = (\tau_i \circ \overline{\omega}_\pi)|_{I_K}^{n_i e_M/(p^f-1)}.$$

Fix any $0 \leqslant j < e$. Recall that $m_{i',j} \equiv n_{\phi_j(i')+kf'} \bmod (p^f-1)$ for any $i' \in \{0, \ldots, f'-1\}$ and $k \in \{0, \ldots, f''-1\}$. Writing $m'_{i',j} := m_{i',j} e_M/(p^f-1)$, it is clear that

$$\chi = \mu(\tau_{\phi_j(i')+kf'} \circ \overline{\omega}_\pi)^{m'_{i',j}}$$

for a unique unramified character $\mu : \mathrm{Gal}(L/K) \to \overline{\mathbf{F}}_p^\times$ independent of i, j.

Recall that we have an isomorphism

$$l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p \cong \bigoplus_{\tau : k \hookrightarrow \overline{\mathbf{F}}_p} l \otimes_{k,\tau} \overline{\mathbf{F}}_p.$$

By the normal basis theorem l is free of rank 1 over $k[\mathrm{Gal}(l/k)]$ and, thus, $l \otimes_{k,\tau} \overline{\mathbf{F}}_p$ is free of rank 1 over $\overline{\mathbf{F}}_p[\mathrm{Gal}(l/k)]$. The latter statement means that $l \otimes_{k,\tau} \overline{\mathbf{F}}_p$ is isomorphic to the regular representation of $\mathrm{Gal}(l/k)$ over $\overline{\mathbf{F}}_p$, which splits up in a direct sum over all characters by Maschke's Theorem. Hence, for each embedding τ, the μ-eigenspace $\Lambda_{\tau,\mu}$ defined as

$$\left\{a \otimes b \in l \otimes_{k,\tau} \overline{\mathbf{F}}_p \;\middle|\; g(a) \otimes b = (1 \otimes \mu(g)) a \otimes b \text{ for all } g \in \mathrm{Gal}(L/K)\right\}$$

is 1-dimensional over $\overline{\mathbf{F}}_p$. We let $\lambda_{\tau,\mu}$ be any non-zero element of $\Lambda_{\tau,\mu}$; note that these elements are linearly independent over $\overline{\mathbf{F}}_p$ for differing embeddings τ.

Then, for any $0 \leqslant j < e$, $0 \leqslant i' < f'$ and $0 \leqslant k < f''$, we define

$$u_{i'+kf',j} := \varepsilon_{\pi^{m'_{i',j}}}(\lambda_{\tau_{\phi_j(i')+kf'},\mu}),$$

which we will abbreviate as

$$u_{i,j} = \varepsilon_{\pi^{m'_{i',j}}}(\lambda_{\tau_{\phi_j(i)},\mu}),$$

where ε_α is defined by (5.2.1). For each $0 \leqslant j < e$, we have exactly f elements $u_{i,j}$. Later we will prove that the elements $u_{i,j}$ will give the explicit basis of U_χ that we are pursuing. In order for this even to make sense, we will now show $u_{i,j} \in U_\chi$. For any $g \in \mathrm{Gal}(M/K)$, it follows from the observation $\omega_\pi(g) = [\overline{\omega}_\pi(g)]$ that

$$g \cdot E([a]\pi^{m'_{i',j}}) = E\left([g(a)\overline{\omega}_\pi(g)^{m'_{i',j}}]\pi^{m'_{i',j}}\right)$$

for any $a \in l$. Thus,

$$\begin{aligned} g \cdot \varepsilon_{\pi^{m'_{i',j}}}(\lambda_{\tau_{\phi_j(i)},\mu}) &= \varepsilon_{\pi^{m'_{i',j}}}((\overline{\omega}_\pi(g)^{m'_{i',j}} \otimes 1)g(\lambda_{\tau_{\phi_j(i)},\mu})) \\ &= \varepsilon_{\pi^{m'_{i',j}}}((\overline{\omega}_\pi(g)^{m'_{i',j}} \otimes \mu(g))\lambda_{\tau_{\phi_j(i)},\mu}). \end{aligned}$$

Since $\overline{\omega}_\pi(g)^{m'_{i',j}} \otimes \mu(g) = 1 \otimes \mu(g)(\tau_{\phi_j(i)} \circ \overline{\omega}_\pi(g))^{m'_{i',j}} = 1 \otimes \chi(g)$ in $l \otimes_{k,\tau_{\phi_j(i)}} \overline{\mathbf{F}}_p$, we see that $gu_{i,j} = (1 \otimes \chi(g))u_{i,j}$ for all $g \in \mathrm{Gal}(M/K)$. Therefore, we can view $u_{i,j}$ as an element of U_χ.

5.2.4. The definitions of u_{triv} and u_{cyc}. The definition of u_{triv} is straightforward. For $g \in \mathrm{Gal}(M/K)$, it is clear that $g(\pi) = \omega_\pi(g)\pi$. As noted above, the image of ω_π is contained in $\mu_{e_M}(K)$. Since p is coprime to e_M, the p-th power map gives an isomorphism $\mu_{e_M}(K) \xrightarrow{\sim} \mu_{e_M}(K)$. Thus, in fact, $\omega_\pi(g) \in (M^\times)^p$ and we set

$$u_{\mathrm{triv}} := \pi \otimes 1 \in M^\times \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p,$$

which is an element of U_χ when χ is the trivial character.

Suppose χ is cyclotomic. Recall from the last part of the proof of Theorem 5.1.1 that we have already proved explicitly that, for $m = \frac{epe_M}{p-1}$, we have

$$\frac{U_m}{(U_m \cap (M^\times)^p)U_{m+1}} \cong \mathbf{F}_p(\chi).$$

However, recall that the p-adic exponential converges on values of $y \in M$ such that $v_M(y) > e_M e/(p-1)$. For $1+x \in U_{m+1}$, we have $v_M(\log(1+x)) > m$ and, thus, we see that $\exp(\log(1+x)/p)$ converges to a p-th root of $1+x$. Therefore, $U_{m+1} \subset (M^\times)^p$ and also $U_{m+1} \subset (U_m \cap (M^\times)^p)$. Thus, we have an injection of the quotient above into $\mathcal{O}_M^\times \otimes_{\mathbf{Z}} \mathbf{F}_p$.

We extend the injection by scalars to $\overline{\mathbf{F}}_p$ and define u_{cyc} to be any nontrivial element of

$$u_{\mathrm{cyc}} \in U_m \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p \hookrightarrow \mathcal{O}_M^\times \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p.$$

It is now obvious from the isomorphism with $\mathbf{F}_p(\chi)$ that for any element $g \in \mathrm{Gal}(M/K)$ we have that

$$g(u_{\mathrm{cyc}}) = (\chi(g) \otimes 1)u_{\mathrm{cyc}} = (1 \otimes \chi(g))u_{\mathrm{cyc}},$$

hence, indeed, $u_{\mathrm{cyc}} \in U_\chi$.

5.3. An explicit basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$

In this section we will prove that the elements as constructed in the previous section give an explicit basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. We will do this by proving the following theorem.

THEOREM 5.3.1. *Let B denote the elements $u_{i,j}$ for $0 \leqslant i \leqslant f-1$ and $0 \leqslant j \leqslant e-1$ with, additionally, the elements u_{triv} if χ is trivial and u_{cyc} if χ is cyclotomic. Then B is an $\overline{\mathbf{F}}_p$-basis of U_χ.*

PROOF. To prove this theorem, we will define a decreasing filtration on U_χ, which is dual to the increasing filtration on $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ defined earlier. Let $\mathrm{Fil}^0 U_\chi = U_\chi$ and let $\mathrm{Fil}^m U_\chi$ denote the image of the map

$$(U_m \otimes \overline{\mathbf{F}}_p(\chi^{-1}))^{\mathrm{Gal}(M/K)} \longrightarrow (M^\times \otimes \overline{\mathbf{F}}_p(\chi^{-1}))^{\mathrm{Gal}(M/K)} =: U_\chi$$

for $m \geqslant 1$. Let $\mathrm{gr}^m U_\chi := \mathrm{Fil}^m U_\chi / \mathrm{Fil}^{m+1} U_\chi$ as usual. It is immediate by duality that $\dim_{\overline{\mathbf{F}}_p} U_\chi = \dim_{\overline{\mathbf{F}}_p} H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. More specifically, whenever $0 < m < \frac{pee_M}{p-1}$ and $p \nmid m$, it follows as in the proof of Theorem 5.1.1 and the discussion in §5.2.2 that

$$\mathrm{gr}^s \left(H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \right) \cong \mathrm{Hom}_{\mathrm{Gal}(M/K)} \left(U_m/U_{m+1}, \overline{\mathbf{F}}_p(\chi) \right),$$

where $s := 1 + \frac{m}{e_M}$. We claim that

$$\mathrm{gr}^m U_\chi \cong \left(U_m/U_{m+1} \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p(\chi^{-1}) \right)^{\mathrm{Gal}(M/K)}.$$

In the proof of Theorem 5.1.1 we show that under these assumptions on m we have that $(M^\times)^p \cap U_m \subset U_{m+1}$. Letting $\overline{U}_i$ denote the image of U_i in $M^\times \otimes \mathbf{F}_p$, we obtain an exact sequence of $\mathbf{F}_p$-modules

$$1 \longrightarrow \overline{U}_{m+1} \longrightarrow \overline{U}_m \longrightarrow U_m/U_{m+1} \longrightarrow 1.$$

The claim for these m now follows by noting that

$$\left(- \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p(\chi^{-1}) \right)^{\mathrm{Gal}(M/K)}$$

is exact since $\mathrm{Gal}(M/K)$ has order prime-to-p. In particular, it follows from this claim that $\dim_{\overline{\mathbf{F}}_p} \mathrm{gr}^m U_\chi = d_s$ for $1 < s := 1 + \frac{m}{e_M} < 1 + \frac{pe}{p-1}$ and d_s as in Theorem 5.1.1.

Since the size of B is equal to the $\overline{\mathbf{F}}_p$-dimension of U_χ, it will suffice to prove that each graded is spanned by a subset of elements of B. By the dimensions of Theorem 5.1.1, we only need to consider integers m such that $d_s > 0$.

The rest of the proof follows from our constructions. If $m = \frac{epe_M}{p-1}$, then it suffices to note u_{cyc} is a non-trivial element of $\mathrm{gr}^m U_\chi = \mathrm{Fil}^m U_\chi$, which is 1-dimensional.

If $0 < m < \frac{epe_M}{p-1}$, then we may assume that $m = m'_{i',j}$ as defined in §5.2.3. The elements

$$u_{i,j} := \varepsilon_{\pi^{m'_{i',j}}}(\lambda_{\tau_{\phi_j(i')+kf'},\mu})$$

for $0 \leqslant k < f''$ are all non-trivial elements of $\mathrm{gr}^m U_\chi$ – this follows, for example, since $E(x) \in 1+x+x^2\mathbf{Z}_p[\![x]\!]$. It suffices to prove that these elements are linearly independent in $\mathrm{gr}^m U_\chi$. Since $p \nmid m$, we showed that

$$\mathrm{gr}^m U_\chi \cong \left(U_m/U_{m+1} \otimes \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M/K)}.$$

Since the map

$$\begin{aligned} l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p &\to U_m/U_{m+1} \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p \\ a \otimes b &\mapsto (1 + [a]\pi^m) \otimes b \end{aligned}$$

induced by ε_{π^m} is an isomorphism and the elements

$$\{\lambda_{\tau_{\phi_j(i')+kf'},\mu} \mid 0 \leqslant k < f''\}$$

are $\overline{\mathbf{F}}_p$-linearly independent in $l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$, we see that their images are as well.

Lastly, if $m = 0$, it suffices to note that $u_{\mathrm{triv}} = \pi \otimes 1$ does not lie in $\mathrm{Fil}^1 U_\chi$. □

Given the basis B above we obtain the dual basis $c_{i,j}$ for $0 \leqslant i \leqslant f-1$ and $0 \leqslant j \leqslant e-1$ with, additionally, c_{ur} and c_{tr} if χ is trivial or cyclotomic. This dual basis must, simply by duality, form a basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ – the subscripts refer to the unramified and très ramifiée part of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$.

Corollary 5.3.2. *The set consisting of the classes $c_{i,j}$ for $0 \leqslant i \leqslant f-1$ and $0 \leqslant j \leqslant e-1$ with, additionally, c_{ur} if χ is trivial and c_{tr} if χ is cyclotomic forms a basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$.*

Once again we emphasise that the explicit basis as defined here may depend on the choice of extension M and the choice of uniformiser π of M in §5.2.2.

CHAPTER 6

Explicit Serre weights over ramified bases

In this chapter we use the explicit basis obtained in the previous chapter to give an explicit definition of the distinguished subspaces L_V defined in §3.3: we will define them as a subspace spanned by a subset of our explicit basis elements. In Theorem 6.3.9 we will prove the equivalence of our subspaces spanned by explicit basis elements with the distinguished subspaces L_V, thereby providing all the necessary theoretical foundation to give a new explicit reformulation of the conjectures on the modularity of mod p Galois representations of totally real number fields.

This chapter owes a great deal to the ideas of the papers [CEGM17] and [GLS15]. In particular, Sections 6.1, 6.2 and 6.3 are direct generalisations of [CEGM17, §3] to the case where K is an arbitrary local field (rather than K being an unramified extension of $\mathbf{Q}_p$). Both our approach and our presentation is, in part, based on their paper; again we invite the curious reader to have a look at [CEGM17] for a comparison.

6.1. Reductions of pseudo-Barsotti Tate representations

One of the essential ingredients in our proof of the equivalence of the two formulations is the classification in [GLS15] of representations that arise as reductions of pseudo-Barsotti–Tate representations. Since we will heavily use their results and their notation, we will quickly recall their most important results adapted to the case at hand. We note that in [GLS15] only the case $p > 2$ is covered. We will use Wang's extension [Wan17] of their results to $p = 2$ for the remaining case.

6.1.1. Field of norms and étale φ-modules. Let us very briefly recall the theory of the field of norms and étale φ-modules. We were given a local field K and a fixed uniformiser π_K. We emphasise that our choices of uniformiser in this section and in the previous sections must be compatible. We define a compatible system of p^nth roots of our uniformiser as follows: let $\pi_0 = -\pi_K$. We define π_n inductively for any $n > 0$ as a pth root of π_{n-1}, that is, satisfying $\pi_n^p = \pi_{n-1}$. Let $K_n := K(\pi_n)$ and $K_\infty = \bigcup_{n=0}^{\infty} K_n$. If $p = 2$, then we assume that our uniformiser π_K was chosen to satisfy

[Wan17, Lem. 2.1]; that is, we assume $K_\infty \cap K_{p^\infty} = K$, where we define $K_{p^\infty} := \bigcup_{n\geqslant 1} K(\zeta_{p^n})$ with ζ_{p^n} a primitive p^n-th root of unity. The theory of the field of norms lets us identify

$$\begin{aligned} k((u)) &\xrightarrow{\ \sim\ } \varprojlim_{N_{K_{n+1}/K_n}} K_n \\ u &\longmapsto (\pi_n)_n, \end{aligned}$$

where the transition maps in the limit are the norm maps. This construction extends to extensions of these fields and we get a natural isomorphism of absolute Galois groups $G_{k((u))} = G_{K_\infty}$. On the other hand there exists an equivalence of abelian categories between the category of finite-dimensional $\overline{\mathbf{F}}_p$-representations of $G_{k((u))}$ and the category of **étale φ-modules**. These are finite $k((u)) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$-modules $\mathcal{M}$ equipped with a φ-semilinear map $\varphi\colon \mathcal{M} \to \mathcal{M}$ such that the induced $k((u)) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$-linear map $\varphi^*\mathcal{M} \to \mathcal{M}$ is an isomorphism. The functor T from étale φ-modules to representations of $G_{k((u))}$ is given by

$$T\colon \mathcal{M} \to \left(k((u))^{\mathrm{sep}} \otimes_{k((u))} \mathcal{M}\right)^{\varphi=1}.$$

The isomorphism $k \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p \to \prod_{i=0}^{f-1} \overline{\mathbf{F}}_p$ gives a decomposition $\mathcal{M} = \prod_i \mathcal{M}_i$, where φ now induces $\overline{\mathbf{F}}_p$-linear morphisms $\varphi\colon \mathcal{M}_{i-1} \to \mathcal{M}_i$. We will make use of this theory by describing finite-dimensional $\overline{\mathbf{F}}_p$-representations of G_{K_∞} via étale φ-modules.

6.1.2. The structure theorem of Gee–Liu–Savitt. From now on let us fix a Serre weight $V = V_{\underline{\alpha},\underline{0}}$ and a pair of characters $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$ as in §3.3.2. (Recall that we were free to assume that V is of the form $V_{\underline{\alpha},\underline{0}}$, since we can obtain the case of a general Serre weight from this one by twisting.) We will write L_V for $L_{V_{\underline{\alpha},\underline{0}}}(\chi_1, \chi_2)$ and we will assume this is non-empty. Recall that we defined the integers $r_i \in [1, p]$ via $r_i := \alpha_i + 1$ and we write $\chi := \chi_1\chi_2^{-1}$. For any $0 \leqslant i < f$, we may decompose χ as a power of ω_i and an unramified character μ independent of i. Then μ factors as a character $\mu : \mathrm{Gal}(L/K) \to \overline{\mathbf{F}}_p^\times$ for some finite unramified extension L of K of prime-to-p order.

First we need to get rid of an exceptional pathological case. Later we will define the subspaces L_V^{AH} using our constructed basis and we will claim $L_V^{\mathrm{AH}} = L_V$ as defined above. Before we continue let us define this space in one exceptional case.

DEFINITION 6.1.1. If χ is cyclotomic, χ_2 is unramified and $r_i = p$ for all $0 \leqslant i < f$, then we define

$$L_V^{\mathrm{AH}}(\chi_1, \chi_2) := H^1(G_K, \overline{\mathbf{F}}_p(\chi)).$$

Note that it follows from the last part of the proof [GLS15, Thm. 6.1.8] that if χ is cyclotomic, χ_2 is unramified and $r_i = p$ for all i, then

$$L_V(\chi_1, \chi_2) = H^1(G_K, \overline{\mathbf{F}}_p(\chi)),$$

so in this exceptional case we indeed have that $L_V^{\mathrm{AH}}(\chi_1, \chi_2) = L_V(\chi_1, \chi_2)$.

We will from now on assume that if χ is cyclotomic and χ_2 is unramified, then $r_i < p$ for at least one i. This assumption has the consequence that the restriction map

$$\mathrm{res} : H^1(G_K, \overline{\mathbf{F}}_p(\chi)) \to H^1(G_{K_\infty}, \overline{\mathbf{F}}_p(\chi))$$

becomes injective when restricted to L_V – this is [GLS15, Lem. 5.4.2] for χ non-cyclotomic and follows from the proof of [GLS15, Thm. 6.1.8] when χ is cyclotomic. (Note that it follows from Wang [Wan17] that these results also work for $p = 2$.) Alternatively, the injectivity for χ cyclotomic follows from the fact that under the assumption L_V is contained in the peu ramifié subspace of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ by Theorem 4.1.1. By [GLS15, Lem. 5.4.2] the kernel of the restriction map is the très ramifiée line spanned by the fixed uniformiser $-\pi_K$. Therefore, the restriction map is injective on this subspace. Since we are excluding the case above, we are free to restrict our representations to G_{K_∞} from now on and talk about the corresponding étale φ-modules.

6.1.2.1. *The integers* t_i, s_i. Before we state the main theorem of [GLS15], we need to introduce just a little more notation: we need to introduce the integers t_i, s_i corresponding to the maximal and minimal Kisin modules of [GLS15, §5.3]. We will take an ad hoc approach. Write $\chi_2|_{I_K} = \prod_i \omega_i^{m_i}$ for the uniquely determined integers $m_i \in [0, p-1]$ with not all m_i equal to $p-1$. Now let $\mathcal{S}$ be the set of f-tuples of non-negative integers $(a_0, \ldots, a_{f-1})$ satisfying $\chi_2|_{I_K} = \prod_i \omega_i^{a_i}$ and $a_i \in [0, e-1] \cup [r_i, r_i + e - 1]$ for all i. This set is non-empty by our assumption that L_V is non-empty. If we write v_i for the f-tuple $(0, \ldots, -1, p, \ldots, 0)$ with the -1 in the ith position and v_{f-1} for $(p, 0, \ldots, 0, -1)$, then it is proved in [GLS15, Lem. 5.3.1] that there exists a subset $J \subseteq \{0, \ldots, f-1\}$, possibly empty, such that

$$(m_0, \ldots, m_{f-1}) + \sum_{i \in J} v_i \in \mathcal{S}$$

and we can choose $J = J_{\min}$ minimal in the sense that it is contained in any other subset satisfying this requirement. Then we define

$$(t_0, \ldots, t_{f-1}) := (m_0, \ldots, m_{f-1}) + \sum_{i \in J_{\min}} v_i \in \mathcal{S}.$$

We will define $s_i := (r_i + e - 1) - t_i$ for all i. Note that it follows from our construction that $s_i, t_i \in [0, e-1] \cup [r_i, r_i + e - 1]$ and $s_i + t_i = r_i + e - 1$ for all i.

6.1.2.2. *The main structure theorem of Gee–Liu–Savitt.* We will understand $(a)_i$ to mean the following: $(a)_i = a$ if $i \equiv 0 \bmod f$ and $(a)_i = 1$ otherwise. Now we are ready to state the main structure theorem of [GLS15].

THEOREM 6.1.2. *The image of the subspace L_V of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ after restriction to $H^1(G_{K_\infty}, \overline{\mathbf{F}}_p(\chi))$ consists precisely of those classes that can be represented by étale φ-modules $\mathcal{M}$ of the following form: we can choose bases e_i, f_i of $\mathcal{M}_i$ for which φ has the form*

$$\varphi(e_{i-1}) = u^{t_i} e_i;$$
$$\varphi(f_{i-1}) = (a)_i u^{s_i} f_i + y_i e_i,$$

where $a = \mu(\mathrm{Frob}_K)$ and $y_i \in \overline{\mathbf{F}}_p[\![u]\!]$ is a polynomial of which the degrees of the non-zero terms lie in the interval

- $[0, s_i - 1]$ *if $t_i \geqslant r_i$ except, possibly, if χ is trivial;*
- $\{t_i\} \cup [r_i, s_i - 1]$ *if $t_i < r_i$ except, possibly, if χ is trivial.*
- *If χ is trivial, we make any single choice of $i_0 \in [0, \ldots, f-1]$ and for i_0 in addition to the intervals defined above we also allow terms of degree*

$$\left\{ s_{i_0} + \frac{1}{p^f - 1} \sum_{k=1}^{f} p^{f-k}(s_{i_0+k} - t_{i_0+k}) \right\}.$$

In every case the polynomials y_i are uniquely determined by $\mathcal{M}$ and every collection of polynomials subject to the conditions above corresponds to a class in L_V.

PROOF. For $p > 2$, the statement of [GLS15, Thm. 5.1.5] shows that the corresponding Kisin modules (which are just lattices in $\mathcal{M}$) have the form above. It follows from [GLS15, §5] in the non-cyclotomic case and [GLS15, §6] in the cyclotomic case that we get the full subspace L_V, since we chose the t_i and s_i to be minimal and maximal, respectively. In the non-cyclotomic case it follows from the proof of [GLS15, Thm. 5.4.1] that the corresponding elements of $H^1(G_{K_\infty}, \overline{\mathbf{F}}_p(\chi))$ (and hence the corresponding étale φ-modules) are uniquely determined by y_i and that any collection of polynomials $\{y_i\}$ satisfying the conditions above corresponds to a class in L_V. In the cyclotomic case (under the assumption that we are not in the exceptional case above) the proof of [GLS15, Thm. 6.1.8] gives the same uniqueness and existence result. It follows from Wang [Wan17] that the results from [GLS15] quoted here and their proofs carry over naturally to $p = 2$ (assuming we have carefully chosen our uniformiser of K) giving the required result in this case as well. $\square$

Definition 6.1.3. Given $\{r_i, t_i, s_i \mid 0 \leqslant i < f\}$ as defined at the beginning of §6.1.2 and in §6.1.2.1, we define

- $\mathcal{I}_i := [0, s_i - 1]$ if $t_i \geqslant r_i$;
- $\mathcal{I}_i := \{t_i\} \cup [r_i, s_i - 1]$ if $t_i < r_i$.

Here we have simply given the intervals appearing in the theorem a name for later convenience. We note that (both in the definition and the theorem) we follow standard conventions and let $\mathcal{I}_i := \varnothing$ if $t_i \geqslant r_i$ and $s_i = 0$, whereas, if $t_i < r_i$ and $s_i = r_i$, we let $\mathcal{I}_i := \{t_i\}$.

6.2. Restricting to G_{M_∞}

In this section we will use the structure theorem of [GLS15] from the previous section to find the image of L_V (after restricting to G_{M_∞}) in terms of Artin–Schreier theory. Later we will use an explicit reciprocity law (see Theorem 6.3.1) to compare the Artin–Schreier theoretic image of L_V to our explicit basis elements of the previous chapter.

Recall that we let $M = L(\pi)$ be a totally tamely ramified extension of an unramified extension L/K of degree prime-to-p, where the uniformiser π of M is a solution of $x^{e_M} + \pi_K = 0$ for $e_M \mid p^f - 1$ and we take M sufficiently large so that $\chi|_{G_M}$ is trivial. We will denote the residue field of M by l.

Since e_M and p are coprime, we have that for each $n \geqslant 1$ there is a unique p^nth root π^{1/p^n} of π that satisfies $(\pi^{1/p^n})^{e_M} = \pi_n$, i.e. the choice of p^nth root of π is compatible with the choice of p^nth root of $-\pi_K$ in the definition of K_∞. Let $M_n := M(\pi^{1/p^n})$ and $M_\infty = \bigcup_{n \geqslant 0} M_n$. It follows by the theory of the field of norms and local class field theory applied to $l((u))$ that

$$\mathrm{Gal}\left(M_\infty^{(p)}/M_\infty\right) \simeq \mathrm{Gal}\left(l((u))^{(p)}/l((u))\right) \simeq l((u))^\times \otimes \mathbf{F}_p,$$

where, for any field F, we write $F^{(p)}$ for the maximal exponent p abelian extension of F. Furthermore, if we let $\psi : l((u))^{\mathrm{sep}} \to l((u)^{\mathrm{sep}}$ denote the Artin–Schreier map defined by $\psi(x) = x^p - x$, then Artin–Schreier theory gives an isomorphism

$$H^1(G_{M_\infty}, \overline{\mathbf{F}}_p) = H^1(G_{l((u))}, \overline{\mathbf{F}}_p) \cong (l((u))/\psi l((u))) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p. \tag{6.2.1}$$

By [Ser79, Ch. X, §3] the element $a \in l((u))$ concretely corresponds to the homomorphism $f_a : G_{l((u))} \to \mathbf{F}_p$ given by $f_a(g) = g(x) - x$, where $x \in l((u))^{\mathrm{sep}}$ is chosen so that $\psi(x) = a$. Any two-dimensional $\overline{\mathbf{F}}_p$-representation ρ of $G_{l((u))}$ that arises as the extension of a character χ by itself corresponds naturally to a cocyle in $H^1(G_{l((u))}, \overline{\mathbf{F}}_p)$ via the standard isomorphism

$$\begin{gathered} \mathrm{Ext}_{\mathrm{Rep}_{\overline{\mathbf{F}}_p}(G_{l((u))})}(\chi, \chi) \to H^1(G_{l((u))}, \overline{\mathbf{F}}_p), \\ \rho \cong \chi \otimes \begin{pmatrix} \mathbf{1} & c_\rho \\ 0 & \mathbf{1} \end{pmatrix} \mapsto [\sigma \mapsto c_\rho(\sigma)]. \end{gathered} \tag{6.2.2}$$

Since M/K is an extension of degree prime-to-p, so is M_∞/K_∞. Therefore, the restriction map $H^1(G_{K_\infty}, \overline{\mathbf{F}}_p(\chi)) \to H^1(G_{M_\infty}, \overline{\mathbf{F}}_p)$ is injective and we may describe L_V completely by its image in $H^1(G_{M_\infty}, \overline{\mathbf{F}}_p)$ or by the classes corresponding to this image via Artin-Schreier theory, which is what we will do.

If $\mathcal{M}$ is an étale φ-module with corresponding G_{K_∞}-representation denoted by $T(\mathcal{M})$, then it is easy to check that the étale φ-module corresponding to $T(\mathcal{M})|_{G_{M_\infty}}$ is

$$\mathcal{M}_M := l((u)) \otimes_{k((u)), u \mapsto u^{e_M}} \mathcal{M}.$$

Applying this to one of the étale φ-modules arising in the statement of Theorem 6.1.2, it follows that (with the obvious choice of basis e_i, f_i for $\mathcal{M}_{M,i}$) the matrix of $\varphi : \mathcal{M}_{M,i-1} \to \mathcal{M}_{M,i}$ is

$$\begin{pmatrix} u^{t_i e_M} & y_{i,M} \\ 0 & (a)_i u^{s_i e_M} \end{pmatrix},$$

where we let $y_{i,M} \in \overline{\mathbf{F}}_p[u^{e_M}]$ denote the image of $y_i \in \overline{\mathbf{F}}_p[u]$ under $u \mapsto u^{e_M}$. Here the $\mathcal{M}_{M,i}$ are periodic with period $f[l : k]$, but t_i, s_i and $y_{i,M}$ only depend on $i \bmod f$.

Recall that we defined $a = \mu(\mathrm{Frob}_K)$ and that the unramified character μ factors as $\mu\colon \mathrm{Gal}(L/K) \to \overline{\mathbf{F}}_p^\times$, so that $a^{[l:k]} = 1$. We will try to find a change of basis such that the diagonal entries of $\varphi : \mathcal{M}_{M,i-1} \to \mathcal{M}_{M,i}$ are identical. Since

$$\rho|_{I_K} \sim \begin{pmatrix} \prod_i \omega_i^{s_i} & * \\ 0 & \prod_i \omega_i^{t_i} \end{pmatrix}$$

and $\chi_1^{e_M} = \chi_2^{e_M}$, it follows that $\left(\frac{p^f-1}{e_M}\right)$ divides

$$\sum_{j=0}^{f-1}(s_{i+1+j} - t_{i+1+j})p^{f-1-j}$$

for all i. Hence, we may define integers

$$\alpha_i := \left(\frac{e_M}{p^f-1}\right)\sum_{j=0}^{f-1}(s_{i+1+j} - t_{i+1+j})p^{f-1-j}.$$

If we set $e_i' := u^{\alpha_i}e_i$ and $f_i' = a^{\lfloor i/f\rfloor}f_i$ for $0 \leqslant i \leqslant f[l:k]-1$, then after this change of basis the matrix of $\varphi : \mathcal{M}_{M,i-1} \to \mathcal{M}_{M,i}$ becomes

$$\begin{pmatrix} u^{t_ie_M+p\alpha_{i-1}-\alpha_i} & a^{\lfloor i-1/f\rfloor}y_{i,M}u^{-\alpha_i} \\ 0 & u^{s_ie_M}\end{pmatrix}.$$

That is, upon noting that $t_ie_M + p\alpha_{i-1} - \alpha_i = s_ie_M$, after the change of basis the matrix of $\varphi : \mathcal{M}_{M,i-1} \to \mathcal{M}_{M,i}$ becomes

$$u^{s_ie_M} \otimes \begin{pmatrix} 1 & a^{\lfloor i-1/f\rfloor}y_{i,M}u^{-(s_ie_M+\alpha_i)} \\ 0 & 1\end{pmatrix}$$

for $0 \leqslant i \leqslant f[l:k]-1$. The exponents of u will be important later, so let us give them a name.

DEFINITION 6.2.1. For all $0 \leqslant i < f$, we define the constants

$$\xi_i := (p^f-1)s_i + \sum_{j=0}^{f-1}(s_{i+j+1} - t_{i+j+1})p^{f-1-j}.$$

Note that for the exponent in the matrix above we have that

$$s_ie_M + \alpha_i = \frac{e_M\xi_i}{p^f-1}.$$

In line with our earlier notation, let us therefore write ξ_i' for $\frac{e_M\xi_i}{p^f-1}$.

LEMMA 6.2.2. *We have that* $\xi_i \equiv n_i \bmod p^f-1$ *and, therefore, that* $\xi_i' \equiv \frac{e_Mn_i}{p^f-1} \bmod e_M$ *for all* i.

PROOF. From $\chi|_{I_K} = \chi_1\chi_2^{-1}|_{I_K}$ and Theorem 6.1.2 above, we have that $\prod_i \omega_i^{s_i-t_i} = \omega_i^{n_i}$, that is

$$\sum_{j=0}^{f-1}(s_{i+1+j} - t_{i+1+j})p^{f-1-j} \equiv n_i \bmod p^f-1.$$

But this sum is equal to $\xi_i - s_i(p^f-1)$. ☐

Recall that in Section 5.2.3 we proved that for any embedding $\tau : k \to \overline{\mathbf{F}}_p$ we have that $l \otimes_{k,\tau} \overline{\mathbf{F}}_p$ is free of rank one over $\overline{\mathbf{F}}_p[\mathrm{Gal}(L/K)]$. It follows that the μ-eigenspace $\Lambda_{\tau,\mu}$ defined as

$$\left\{a \otimes b \in l \otimes_{k,\tau} \overline{\mathbf{F}}_p \;\middle|\; g(a) \otimes b = (1 \otimes \mu(g))a \otimes b \text{ for all } g \in \mathrm{Gal}(L/K)\right\}$$

is 1-dimensional over $\overline{\mathbf{F}}_p$. For $a = \mu(\mathrm{Frob}_K)$, we define the non-zero element

$$\lambda_{\tau,\mu} := (1, a^{-1}, \dots, a^{1-[l:k]}) \in l \otimes_{k,\tau} \overline{\mathbf{F}}_p$$

and note that this is in fact a basis of the one-dimensional vector space $\Lambda_{\tau,\mu}$. Here we have used the standard identification

$$\begin{aligned} l \otimes_{k,\tau} \overline{\mathbf{F}}_p &\xrightarrow{\sim} \prod_{\sigma_i} \overline{\mathbf{F}}_p; \\ x \otimes y &\longmapsto (\sigma_i(x)y)_i, \end{aligned}$$

where the sum runs over all k-embeddings $\sigma_i \colon l \hookrightarrow \overline{\mathbf{F}}_p$ such that $\sigma_i|_k = \tau$. Similarly, $\lambda_{\tau,\mu^{-1}} := (1, a, \dots, a^{[l:k]-1}) \in l \otimes_{k,\tau} \overline{\mathbf{F}}_p$ spans $\Lambda_{\tau,\mu^{-1}}$. Using this notation we may define the element

$$(a^{\lfloor i/f \rfloor})_{i=0,\dots,f[l:k]-1} = (\lambda_{\overline{\tau}_i,\mu^{-1}})_{i=0,\dots,f-1} \in l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p.$$

We can consider $\mathcal{M}_M$ as an $l((u)) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$-module with the obvious choice of basis. Then the matrix of $\varphi_{\mathcal{M}_M}$ becomes

$$(u^{s_i e_M})_{i=0,\dots,f-1} \otimes \begin{pmatrix} 1 & (a^{-1}\lambda_{\overline{\tau}_i,\mu^{-1}} y_{i,M} u^{-\xi_i'})_{i=0,\dots,f-1} \\ 0 & 1 \end{pmatrix}.$$

By the equivalence of categories T between étale φ-modules and $\overline{\mathbf{F}}_p$-representations of $G_{l((u))}$ combined with Equations (6.2.1) and (6.2.2), this étale φ-module then corresponds to a class in $l((u))/\psi l((u)) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$. To understand which class exactly, we prove the following proposition.

Proposition 6.2.3. *Suppose $\mathcal{M}$ is an étale φ-module over $l((u))$ such that $\varphi_{\mathcal{M}} : \mathcal{M} \to \mathcal{M}$ is given by the matrix*

$$\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}.$$

Then the image of $\mathcal{M}$ under the isomorphism

$$\mathrm{Ext}^1_{\mathrm{Rep}_{\mathbf{F}_p}(G_{l((u))})}(1,1) \cong l((u))/\psi l((u))$$

is given by (the class of) α.

Remark 6.2.4. Although strictly speaking we only defined étale φ-modules after having extended coefficients to $\overline{\mathbf{F}}_p$, in this proposition we deal with étale φ-modules $\mathcal{M}$ over $l((u))$. These are simply finite $l((u))$-modules with a φ-semilinear map whose linearisation is an isomorphism. Completely analogously, $T(\mathcal{M}) := (l((u))^{\mathrm{sep}} \otimes_E \mathcal{M})^{\varphi=1}$ gives an equivalence of categories of between étale φ-modules and $\mathbf{F}_p$-representations of $G_{l((u))}$.

Proof. To simplify the notation let us write E for $l((u))$ and E_s for its separable closure. To be able to determine the two-dimensional $\mathbf{F}_p$-representation $T(\mathcal{M})$ we will write down a basis of the underlying vector space and then we can see how G_E acts on it.

To determine a basis of $T(\mathcal{M}) := (E_s \otimes_E \mathcal{M})^{\varphi_{E_s}\otimes\varphi_{\mathcal{M}}=1}$ we need to solve the equations

$$\varphi(\lambda_0 e_0 + \lambda_1 e_1) = \lambda_0^p e_0 + \lambda_1^p(\alpha e_0 + e_1) = \lambda_0 e_0 + \lambda_1 e_1$$

for $\lambda_0, \lambda_1 \in E_s$. Hence, clearly we require $\lambda_1 \in \mathbf{F}_p$. So we are left with solving $\lambda_0^p - \lambda_0 = -\lambda_1\alpha$. If $\lambda_1 \neq 0$, then the left and right hand side scale by $\mathbf{F}_p$ in the same way. Therefore, if $\lambda \in E_s$ is a root of $\lambda^p - \lambda = \alpha$, then all solutions are given by $(\lambda_0, 0)$ for $\lambda_0 \in \mathbf{F}_p$ and $(\lambda\lambda_1, \lambda_1)$ for $\lambda_1 \in \mathbf{F}_p$. So an $\mathbf{F}_p$-basis is given by solutions $(1,0)$ and $(\lambda, 1)$ corresponding to the $\mathbf{F}_p$-basis of $T(\mathcal{M})$ given by $(v_0, v_1) := (e_0, \lambda e_0 + e_1)$.

Now we study the action of G_E on $T(\mathcal{M})$. For $\sigma \in G_E$, we have that $\sigma \cdot v_0 := \sigma(1)e_0 = v_0$ and

$$\sigma \cdot v_1 := \sigma(\lambda)e_0 + e_1 = \sigma(\lambda)e_0 + e_1 = v_1 + (\sigma(\lambda) - \lambda)v_0.$$

Since $\mathbf{F}_p$ is fixed by G_E, the representation $T(\mathcal{M})$ is of the form

$$\begin{aligned} G_E &\longrightarrow \mathrm{GL}_2(\mathbf{F}_p) \\ \sigma &\longmapsto \begin{pmatrix} 1 & \sigma(\lambda) - \lambda \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Note that it follows from the defining equation of λ that $\sigma(\lambda) - \lambda \in \mathbf{F}_p$ for any $\sigma \in G_E$.

By definition of the isomorphism of Equation (6.2.2) we see that

$$\begin{aligned} \mathrm{Ext}^1_{\mathrm{Rep}_{\mathbf{F}_p}(G_E)}(\mathbf{1}, \mathbf{1}) &\xrightarrow{\sim} H^1(G_E, \mathbf{F}_p) = \mathrm{Hom}(G_E, \mathbf{F}_p) \\ \left\{ \sigma \mapsto \begin{pmatrix} 1 & \sigma(\lambda) - \lambda \\ 0 & 1 \end{pmatrix} \right\} &\longmapsto [\sigma \mapsto (\sigma(\lambda) - \lambda)]. \end{aligned}$$

Now the class of α in $E/\psi(E)$ corresponds by Equation (6.2.1) (and the short explanation after) to the map $f_\alpha : G_E \to \mathbf{F}_p$ defined by the identity $f_\alpha(\sigma) = \sigma(\lambda) - \lambda$ and, hence, it follows that the class of α in $E/\psi(E)$

corresponds to

$$[\sigma \mapsto (\sigma(\lambda) - \lambda)] \in \mathrm{Hom}(G_E, \mathbf{F}_p),$$

as required. $\square$

After extending coefficients to $\overline{\mathbf{F}}_p$, it follows from the proposition that the Artin-Schreier extension of $l((u))$ corresponding to $T(\mathcal{M}_M)$ above is determined by the element $(\lambda_{\overline{\tau}_i,\mu^{-1}} y_{i,M} u^{-\xi'_i})_{i=0,\dots,f-1}$ – note the absence of a^{-1} because scaling by an element of $\overline{\mathbf{F}}_p^{\times}$ does not change the extension. Therefore, we have proved the following result.

COROLLARY 6.2.5. *The image of L_V in $H^1(G_{M_\infty}, \overline{\mathbf{F}}_p) = \mathrm{Hom}(G_{l((u))}, \overline{\mathbf{F}}_p)$ is spanned by the homomorphisms $f_{y_{i,M}\lambda_{\overline{\tau}_i,\mu^{-1}} u^{-\xi'_i}}$ corresponding via Artin-Schreier theory to the elements*

$$y_{i,M}\lambda_{\overline{\tau}_i,\mu^{-1}} u^{-\xi'_i} \in l((u)) \otimes_{k,\overline{\tau}_i} \overline{\mathbf{F}}_p \subseteq l((u)) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p.$$

More precisely, the image is spanned by homomorphisms corresponding to

$$\lambda_{\overline{\tau}_i,\mu^{-1}} u^{de_M - \xi'_i} \in l((u)) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$$

for all $0 \leqslant i < f$ and all $d \in \mathcal{I}_i$, together with the class $\lambda_{\overline{\tau}_{i_0},\mu^{-1}} u^{d_{i_0} e_M - \xi'_{i_0}}$ for

$$d_{i_0} := s_{i_0} + \frac{1}{p^f - 1} \sum_{k=0}^{f-1} (s_{i_0+1+k} - t_{i_0+1+k}) p^{f-1-k}$$

if χ is trivial.

6.3. An explicit basis of L_V

In this section we would like to compare our description of L_V above to the previously constructed basis elements $c_{i,j}$ and give an explicit description of L_V in this way. To explain our approach we need to introduce some theory first.

We have a pairing $\langle \cdot, \cdot \rangle : H^1(G_{M_\infty}, \overline{\mathbf{F}}_p) \times \mathrm{Gal}(M_\infty^{(p)}/M_\infty) \to \overline{\mathbf{F}}_p$ given by evaluation. Recall that the theory of the field of norms and the local Artin map allowed us to write $\mathrm{Gal}(M_\infty^{(p)}/M_\infty) \simeq l((u))^\times \otimes \mathbf{F}_p$ and that we used Artin-Schreier theory to write $H^1(G_{M_\infty}, \overline{\mathbf{F}}_p) \simeq (l((u))/\psi l((u))) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$. The real advantage is that we can make the pairing explicit now.

THEOREM 6.3.1. *Let $\sigma_b \in \mathrm{Gal}(M_\infty^{(p)}/M_\infty)$ be the Galois element corresponding via the local Artin map to an element $b \in l((u))^\times \otimes \mathbf{F}_p$, and let f_a be the element of $H^1(G_{M_\infty}, \overline{\mathbf{F}}_p)$ corresponding to $a \in (l((u))/\psi l((u))) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$*

via Artin-Schreier theory. Then

$$\langle f_a, \sigma_b \rangle = \mathrm{Tr}_{l\otimes_{\mathbf{F}_p}\overline{\mathbf{F}}_p/\overline{\mathbf{F}}_p}\left(\mathrm{Res}(a \cdot \frac{db}{b})\right),$$

where $\mathrm{Res}(f du)$ *simply means the coefficient of* u^{-1} *in* f*.*

Proof. See [Ser79, XIV, Cor. to Prop. 15]. ☐

Since we already have a description of the image of L_V in $H^1(G_{M_\infty}, \overline{\mathbf{F}}_p)$ and we defined the $c_{i,j} \in H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ as the basis dual to basis elements

$$u_{i,j} \in U_\chi := \left(M^\times \otimes \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M/K)} \subseteq M^\times \otimes \overline{\mathbf{F}}_p,$$

we may hope to get a description of the elements $u_{i,j}$ in $\mathrm{Gal}(M_\infty^{(p)}/M_\infty)$ and look to find conditions under which the pairing of $u_{i,j}$ with L_V vanishes. The local Artin map Art_M^{-1} induces an isomorphism $\mathrm{Gal}(M^{(p)}/M) \simeq M^\times \otimes \mathbf{F}_p$, so by extension by scalars to $\overline{\mathbf{F}}_p$ we get $\mathrm{Art}_M(u_{i,j}) \in \mathrm{Gal}(M^{(p)}/M) \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$.

Lemma 6.3.2. *We have a commutative diagram of pairings*

$$\begin{array}{ccccc} H^1(G_{M_\infty}, \overline{\mathbf{F}}_p) & \times & \mathrm{Gal}(M_\infty^{(p)}/M_\infty) & \longrightarrow & \overline{\mathbf{F}}_p \\ \uparrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{pr}} & & \\ H^1(G_M, \overline{\mathbf{F}}_p) & \times & \mathrm{Gal}(M^{(p)}/M) & \longrightarrow & \overline{\mathbf{F}}_p \end{array}$$

in the sense that $\langle \mathrm{pr}(\alpha), \beta \rangle = \langle \alpha, \mathrm{res}(\beta) \rangle$*, where the pairings are given by evaluation, the map* res *is given by restriction to* G_{M_∞} *and* pr *is given by restricting an automorphism to* $M^{(p)}$*.*

Proof. Since $H^1(G_M, \overline{\mathbf{F}}_p) = \mathrm{Hom}(G_M, \overline{\mathbf{F}}_p)$ (and similarly for M_∞) and the pairings are given by evaluation, this follows from the definitions. ☐

By the lemma above it is enough to consider the pairing of L_V with elements of $\mathrm{Gal}(M_\infty^{(p)}/M_\infty)$ that map to the elements $\mathrm{Art}_M(u_{i,j})$ under pr. To be able to use the explicit reciprocity law of Theorem 6.3.1, we need to use the local class field theory of $l((u))$ and the theory of the field of norms to get an isomorphism $\mathrm{Gal}(M_\infty^{(p)}/M_\infty) \simeq l((u))^\times \otimes \mathbf{F}_p$. From the field of norms identification $l((u)) \simeq \varprojlim_{N_{M_{n+1}/M_n}} M_n$ we get a natural map $\mathrm{pr}_M : l((u)) \to M$ by projecting onto the M-component which is compatible with local class field theory in the following natural way.

LEMMA 6.3.3. *The following diagram commutes*

$$\begin{array}{ccccc} \mathrm{Gal}(M_\infty^{(p)}/M_\infty) & \xrightarrow[f.o.n.]{\sim} & \mathrm{Gal}\left(l((u))^{(p)}/l((u))\right) & \xrightarrow[\mathrm{Art}_{l((u))}^{-1}]{\sim} & l((u))^\times \otimes \mathbf{F}_p \\ \downarrow \mathrm{pr} & & & & \downarrow \mathrm{pr}_M \\ \mathrm{Gal}(M^{(p)}/M) & & \xrightarrow[\mathrm{Art}_M^{-1}]{\sim} & & M^\times \otimes \mathbf{F}_p. \end{array}$$

PROOF. See [CEGM17, Lem. 3.1.5]. □

The missing step is to find elements that project down under pr_M to our previous $u_{i,j}$. Recall that $E(X) \in \mathbf{Z}_p[\![X]\!]$ denotes the Artin-Hasse exponential. Then, for each $r \geqslant 1$, we get a homomorphism

$$\begin{aligned} \varepsilon_{u^r} : l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p &\to l((u))^\times \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p \\ a \otimes b &\mapsto E(au^r) \otimes b \end{aligned}$$

and, analogously to our earlier definitions of $u_{i,j}$ in §5.2.3, we will define

$$\tilde{u}_{i,j} := \varepsilon_{u^{m'_{i',j}}}(\lambda_{\tau_{\phi_j(i)},\mu}).$$

PROPOSITION 6.3.4. *Under the map* $\mathrm{pr}_M : l((u))^\times \otimes \mathbf{F}_p \to M^\times \otimes \mathbf{F}_p$, *we have that*

$$\mathrm{pr}_M\left(E(au^r)\right) = E([a]\pi^r)$$

for any $r \geqslant 1$ *which is prime to* p. *In particular, after extending by scalars to* $\overline{\mathbf{F}}_p$, *we have that* $\mathrm{pr}_M(\tilde{u}_{i,j}) = u_{i,j}$.

PROOF. To see why this is true, we recall that addition in $\varprojlim M_n$ is defined by the formula

$$(x+y)^{(n)} = \lim_{m\to\infty} N_{M_{n+m}/M_n}(x^{(n+m)} + y^{(n+m)}).$$

If we write $E(X) = \sum_{k\geqslant 0} c_k X^k \in \mathbf{Z}_p[\![X]\!]$, then we see that

$$\begin{aligned} \overline{E}(au^r) &= \overline{E}\left(([a]\pi^r, ([a]\pi^r)^{1/p}, ([a]\pi^r)^{1/p^2}, \dots)\right) \\ &= \sum_{k\geqslant 0} \overline{c}_k \left([a]\pi^r, ([a]\pi^r)^{1/p}, ([a]\pi^r)^{1/p^2}, \dots\right)^k \\ &\mapsto \lim_{m\to\infty} N_{M_m/M}(\sum_{k\geqslant 0} c_k([a]\pi^r)^{k/p^m}), \end{aligned}$$

where we have taken the projection onto the M-component in the last line. Now the proposition follows immediately from [CEGM17, Lem. 3.5.1], where it is proved that for any $n > 1$, $a \in l$ and $r \geqslant 1$ such that $(r,p) = 1$ we have

$$N_{M_n/M} E([a^{1/p^n}](\pi^{1/p^n})^r) = E([a]\pi^r).$$

The second claim follows since all the $m'_{i',j}$ are coprime to p. □

Now we have covered all the theory to state and prove our explicit version of the space L_V in terms of the basis elements constructed previously for $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. In the following definition we will give the definition of an indexing set J_V^{AH} of a subset of embeddings such that the span of basis elements $c_{i,j}$ over this indexing set will give us L_V.

Definition 6.3.5. We let $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ denote the set of all pairs (i, j) in $\mathbf{Z}/f\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}$ for which there exist integers $0 \leqslant k < f$, $d \in \mathcal{I}_k$ and $m \geqslant 0$ such that

1) $p^m m'_{i',j} = \xi'_k - de_M$ and
2) $\phi_j(i) \equiv k - m \bmod f$.

Note that, even though we need to calculate the integers s_i, t_i corresponding to minimal and maximal Kisin modules to be able to define ξ_i and $\mathcal{I}_i$ concretely, these integers can be calculated completely explicitly (as we have done above) without the use of any p-adic Hodge theory. The dependence on $\{r_i\}$ or, equivalently, the dependence on the Serre weight $V_{\underline{\alpha},\underline{0}}$ for $\alpha_i = r_i - 1$ is implicit in the definitions of s_i, t_i (hence ξ_i) and $\mathcal{I}_i$.

Proposition 6.3.6. $\left|J_V^{\mathrm{AH}}(\chi_1, \chi_2)\right| \leqslant \sum_{k=0}^{f-1} |\mathcal{I}_k|$.

Proof. By multiplying the left and right hand sides of the first equation in Definition 6.3.5 by $(p^f - 1)/e_M$, we obtain the equation

$$p^m m_{i',j} = \xi_k - d(p^f - 1); \tag{6.3.1}$$

this follows from the definitions of $m'_{i',j}$ and ξ'_k. Therefore, given a pair (i, j) as in Definition 6.3.5, we can solve the first equation of this definition for some k, d and m if and only if we can solve Equation 6.3.1 for the same k, d and m. It follows that we may assume without loss of generality that $e_M = p^f - 1$.

For a fixed choice of $0 \leqslant k < f$ and $d \in \mathcal{I}_k$, we set $m := v_p(\xi_k - d(p^f - 1))$ and define

$$a := \frac{\xi_k - d(p^f - 1)}{p^m}.$$

It follows from Lemma 6.2.2 that $p^m a \equiv n_k \bmod (p^f - 1)$, so

$$a \equiv n_{k-m} \bmod (p^f - 1).$$

Therefore, by definition of the integers $m_{i',j}$, the first equation of Definition 6.3.5 will have a solution for some $(i, j) \in \mathbf{Z}/f\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}$ if and only if $0 < a < \frac{pe}{p-1}(p^f - 1)$. Suppose that this is the case. Then we have a unique $m_{i',j}$ solving the equation, namely $m_{i',j} = a$. Since the integers $m_{i',j}$ are distinct, this means that (i,j) exists and is unique up to i in the congruence class of $k-m \bmod f'$. The second equation of Definition 6.3.5 requires that $\phi_j(i) \equiv k-m \bmod f$, thereby determining (i,j) uniquely. In other words, we have proved that there exists a unique $(i,j) \in J_V^{\mathrm{AH}}(\chi_1,\chi_2)$ corresponding to our fixed choice of (k,d) if

$$0 < \frac{\xi_k - d(p^f-1)}{p^m} < \frac{ep}{p-1}(p^f-1)$$

and no (i,j) corresponding to (k,d) otherwise. $\square$

We remark that it is possible to show with a direct argument, which carefully uses the minimality (resp. maximality) of the integers t_i (resp. s_i), that the inequalities on a in the proof above are always satisfied. This also follows as a consequence of Theorem 6.3.9 which implies that $\left|J_V^{\mathrm{AH}}(\chi_1,\chi_2)\right| = \sum_{k=0}^{f-1} |\mathcal{I}_k|$.

Let $c_{i,j}$ denote the basis elements of $H^1(G_K,\overline{\mathbf{F}}_p(\chi))$ defined earlier, where we assume we define these making the same choices in the definition of $M = L(\pi)$ as in the current section, that is, they are defined using the same fixed uniformiser $\pi_K \in K$, the same unramified extension L of K and the same π satisfying $\pi^{e_M} + \pi_K = 0$.

Definition 6.3.7. We define $L_V^{\mathrm{AH}}(\chi_1,\chi_2)$ to be the span of

$$\{c_{i,j} \mid (i,j) \in J_V^{\mathrm{AH}}(\chi_1,\chi_2)\}$$

together with c_{un} if χ is trivial and c_{tr} if χ is cyclotomic, χ_2 unramified and $r_i = p$ for all i.

Corollary 6.3.8. $\dim_{\overline{\mathbf{F}}_p} L_V^{\mathrm{AH}}(\chi_1,\chi_2) \leqslant \dim_{\overline{\mathbf{F}}_p} L_V(\chi_1,\chi_2)$.

Proof. This follows immediately from the definitions, Proposition 6.3.6 and Theorem 6.1.2 (since y_i uniquely determines $\mathcal{M}$ and vice-versa). $\square$

Theorem 6.3.9. $L_V(\chi_1,\chi_2) = L_V^{\mathrm{AH}}(\chi_1,\chi_2)$.

Proof. By Corollary 6.3.8 it is enough to prove $L_V \subseteq L_V^{\mathrm{AH}}$. We defined L_V^{AH} in terms of the basis elements $c_{i,j}$ dual to $u_{i,j}$, so we need to prove that the image of every class of L_V in $H^1(G_M,\overline{\mathbf{F}}_p)$ is orthogonal to the elements $\mathrm{Art}_M(u_{i,j})$ in $\mathrm{Gal}(M^{(p)}/M)$ for $(i,j) \notin J_V^{\mathrm{AH}}$ under the pairing of Lemma 6.3.2. If χ is cyclotomic, we also need to prove orthogonality under pairing with u_{cyc}, which we will do first.

If χ is cyclotomic, then the classes that are orthogonal to u_{cyc} are exactly the peu ramifiées classes. We see this, for example, because the subspace orthogonal to u_{cyc} is spanned by the basis elements $\{c_{i,j} \mid 0 \leqslant i < f, 0 \leqslant j < e\}$

and c_{ur} if χ is trivial. Since c_{tr} spans the one-dimensional subspace defined as $\mathrm{Fil}^{1+\frac{ep}{p-1}} H^1(G_K, \overline{\mathbf{F}}_p(\chi))$, it follows that these basis elements span the space $\mathrm{Fil}^{<1+\frac{ep}{p-1}} H^1(G_K, \overline{\mathbf{F}}_p(\chi))$, which equals the peu ramifié subspace by Corollary 4.4.1. However, since we excluded the exceptional case in which L_V equals $H^1(G_K, \overline{\mathbf{F}}_p)$, we have that L_V is always contained in the peu ramifié subspace of $H^1(G_K, \overline{\mathbf{F}}_p)$ by Theorem 4.1.1. Therefore, L_V is always contained in the subspace orthogonal to u_{cyc}.

As outlined above we apply the explicit reciprocity law of Theorem 6.3.1 to the elements $\tilde{u}_{i,j}$ and the elements of Corollary 6.2.5. We must show that for all $0 \leqslant k < f$, $d \in \mathcal{I}_k$ and $(i,j) \notin J_V^{\mathrm{AH}}$

$$\mathrm{Tr}_{l\otimes_{\mathbf{F}_p}\overline{\mathbf{F}}_p/\overline{\mathbf{F}}_p}\mathrm{Res}\left(\mathrm{dlog}(\tilde{u}_{i,j}) \cdot \lambda_{\tau_k,\mu^{-1}} u^{de_M - \xi'_k}\right) = 0$$

and if $\chi = 1$ we also need to show that the pairing with $\lambda_{\overline{\tau}_{i_0},\mu^{-1}} u^{d_{i_0} e_M - \xi'_{i_0}}$ vanishes. Since

$$\mathrm{dlog}E(X) = (X + X^p + X^{p^2} + \dots)\mathrm{dlog}X$$

and $\mathrm{dlog}(\lambda u^n) = n \cdot u^{-1}$, the pairing evaluates to

$$\mathrm{Tr}_{l\otimes_{\mathbf{F}_p}\overline{\mathbf{F}}_p/\overline{\mathbf{F}}_p}\mathrm{Res}\left(\sum_{m\geqslant 0} m'_{i',j}\mathrm{Frob}^m(\lambda_{\tau_{\phi_j(i)},\mu}) u^{m'_{i',j}p^m - 1} \cdot \lambda_{\tau_k,\mu^{-1}} u^{de_M - \xi'_k}\right),$$

where $\mathrm{Frob} : l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p \to l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$ is induced by the p-th power map on l. The residue is given by the coefficient of u^{-1}, hence this can only possibly be non-zero when $p^m m'_{i',j} = \xi'_k - de_M$ for some $m \geqslant 0$. If $\chi = 1$ we must also consider $p^m m'_{i',j} = \xi'_{i_0} - d_{i_0} e_M$, but it follows easily from the observation $\xi'_{i_0} = d_{i_0} e_M$ that this can never have solutions. In the former case, if such an m exists, then the pairing evaluates to

$$m'_{i',j}\mathrm{Tr}_{l\otimes_{\mathbf{F}_p}\overline{\mathbf{F}}_p/\overline{\mathbf{F}}_p}\left(\mathrm{Frob}^m(\lambda_{\tau_{\phi_j(i)},\mu}) \cdot \lambda_{\tau_k,\mu^{-1}}\right).$$

Since

$$\mathrm{Frob}^m(\lambda_{\tau_{\phi_j(i)},\mu}) \cdot \lambda_{\tau_k,\mu^{-1}} = \mathrm{Frob}^m(\lambda_{\tau_{\phi_j(i)},\mu} \cdot \lambda_{\tau_{k-m},\mu^{-1}}),$$

we find that this expression is non-zero if and only if $\tau_{\phi_j(i)} = \tau_{k-m}$, i.e. when $\phi_j(i) \equiv k - m \bmod f$.

In conclusion, we have proved that the pairing of $u_{i,j}$ with L_V is non-zero when there exist integers $0 \leqslant k < f$, $d \in \mathcal{I}_k$ and $m \geqslant 0$ such that

1) $p^m m'_{i',j} = \xi'_k - de_M$ and
2) $\phi_j(i) \equiv k - m \bmod f$.

These are precisely the conditions that imply that $(i,j) \in J_V^{\mathrm{AH}}$, as required. $\square$

COROLLARY 6.3.10. *The space $L_V^{\mathrm{AH}}(\chi_1, \chi_2)$ is independent of the choice of the extension M of K and the choice of the uniformiser π of M.*

PROOF. This follows immediately since $L_V(\chi_1, \chi_2)$ is independent of the choices and we have just proved that $L_V^{\mathrm{AH}}(\chi_1, \chi_2) = L_V(\chi_1, \chi_2)$ for any suitable set of choices. $\square$

CHAPTER 7

Explicit Formulae

In this chapter we report on results (some of which are still conjectural) regarding the search for an explicit formula replacing Definition 6.3.5. That is, given a fixed local field $K/\mathbf{Q}_p$ with ramification degree e and residue degree f and given a pair of characters $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$, we would like to find a formula that takes as input the quantities r_i, s_i and t_i for $i = 0, \ldots, f-1$ and outputs all pairs $(i, j) \in \mathbf{Z}/f\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}$ such that $(i, j) \in J_V^{\mathrm{AH}}(\chi_1, \chi_2)$. Such an explicit formula is given in [DDR16] under the assumption that $K/\mathbf{Q}_p$ is unramified.

In §7.1 we will first give generalisations of §4 and §6 of [DDR16] to the case of an arbitrary local field K which is finite over $\mathbf{Q}_p$. This will give us theoretical results helping to give some indication of what a formula might look like. In §7.2 we will recall the formula given in [DDR16] in case that K is unramified over $\mathbf{Q}_p$. In §7.3 we prove an explicit form of the formula assuming K is totally ramified over $\mathbf{Q}_p$. Lastly, in §7.4 and §7.5 we will give some conjectural formulae under other simplifying assumptions.

The reader will discover that this chapter consists for a large part of combinatorial arguments. Indeed, every time a potential formula is found it seems to boil down to an (often complicated) combinatorial argument to prove the equivalence with Definition 6.3.5. It is, therefore, more a consequence of a lack of time than a lack of mathematical resources that some of the results in §7.4 and §7.5 remain conjectural: the author is convinced that all these results are true and provable with current methods. Whether a formula exists in complete generality is much more debatable. The first problem that arises is that the author was so far unable to find a natural way of defining the integers $m_{i,j}$ in complete generality – natural in the sense that they behave well under the dependencies of §7.1. Without such a natural definition the effort to find a formula seems bound to be hopeless. It may be that a new approach is needed to solve this problem in complete generality.

In this chapter most results (unless stated otherwise) are due to the author although in §7.1 we follow the general approach of [DDR16, §4,§6].

In §7.2 we present no original results, but rather we will recall arguments given in [DDR16] and [CEGM17] for a more complete picture.

For simplicity we will assume $p > 2$ in this chapter.

7.1. Choice-independent subspaces

In this section we will first prove certain properties of the Artin–Hasse exponential. Then we will use these properties to find a combinatorial criterion under which the span of a given subset of our standard basis elements $c_{i,j}$ (as defined in §5.3) is independent from the choice of uniformiser π_K of K and the extension M in their definition. Of course, we already know by Corollary 6.3.10 that the spans L_V^{AH} are independent of choice. However, finding a direct criterion on the basis elements will help us in our search for an explicit formula later. These sections are direct generalisations of §4 and §6 from [DDR16] to the case where K is an arbitrary extension of $\mathbf{Q}_p$. We are grateful to Kracht for making her PhD thesis [Kra11] publicly available. Without this resource we would have never been able to find the essential Proposition 7.1.1 of [Bla05] below.

7.1.1. The Artin-Hasse Exponential. Let p be an odd prime. Recall that the **Artin-Hasse exponential** is given by

$$E_p(x) = \exp\left(\sum_{n\geqslant 0} \frac{x^{p^n}}{p^n}\right).$$

Then $E_p(x)$ is an element of $\mathbf{Z}_p[\![x]\!]$ and $E_p(x) \equiv 1 + x \bmod (x^2)$. Since p is fixed throughout, we will write $E(x)$ instead of $E_p(x)$ from now on.

7.1.1.1. *An additive formula for $E(x)$.* Similarly to the well known identity $\exp(x)\exp(y) = \exp(x+y)$, we may hope to find a formula for $E(x)E(y)$. Indeed such a formula exists, although we need to recall some basic facts about the theory of Witt vectors before we can state it. For a more complete account of this theory see [Ser79, §II.6]. Let $X = (X_0, X_1, X_2, \dots)$ and $Y = (Y_0, Y_1, Y_2, \dots)$ be sequences of commuting indeterminates with $\mathbf{Q}$-coefficients. Recall that the Witt polynomials for $n \geqslant 0$ are given by

$$w_n(X) := w_n(X_0, \dots, X_n) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^n X_n.$$

It is a famous theorem in the theory of Witt vectors that there exist unique polynomials $s_n(X;Y) := s_n(X_0, X_1, \dots, X_n; Y_0, Y_1, \dots, Y_n)$ with $\mathbf{Z}$-coefficients such that, for all n,

$$w_n(s_0(X;Y), s_1(X;Y), \dots, s_n(X;Y)) = w_n(X) + w_n(Y).$$

With a straightforward calculation one finds, for example, that

$$s_0(X_0, Y_0) = X_0 + Y_0;$$

$$s_1(X_0, X_1; Y_0, Y_1) = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} X_0^{p-i} Y_0^i.$$

We will from now on write $S_n(X_0, Y_0) := s_n(X_0, 0, \ldots, 0; Y_0, 0, \ldots, 0)$. The polynomial S_n is then always a homogeneous polynomial of degree p^n.

PROPOSITION 7.1.1. *In* $\mathbf{Z}_p[\![x, y]\!]$ *we have the following equality of formal power series*

$$E(x)E(y) = \prod_{k \geqslant 0} E(S_k(x, y)) = E(x + y) \prod_{k \geqslant 1} E(S_k(x, y)).$$

PROOF. See [Bla05, Lem. 2.4]. $\square$

LEMMA 7.1.2. *In* $\mathbf{Z}[x]$ *we have that, for any* $n \geqslant 0$,

$$S_n(1 + x, -1) \equiv x \bmod (x^2).$$

PROOF. This is clearly true for $S_0(1 + x, -1) = x$. Suppose inductively that it is true for $S_i(1 + x, -1)$ for all $i < n$. By this hypothesis $S_i(1 + x, -1)^{p^{n-i}} \equiv 0 \bmod (x^2)$ for $i < n$. The result follows immediately from the defining equation of $S_n(1 + x, -1)$:

$$S_0(1+x, -1)^{p^n} + pS_1(1+x, -1)^{p^{n-1}} + \cdots + p^n S_n(1+x, -1) = (1+x)^{p^n} - 1.$$

$\square$

COROLLARY 7.1.3. *We can find polynomials* $f_1(x), f_2(x), \ldots \in 1 + x\mathbf{Z}[x]$ *such that in* $\mathbf{Z}_p[\![x, y]\!]$ *we have the equality of formal power series*

$$E((1 + x)y)E(-y) = E(xy) \prod_{k \geqslant 1} E(f_k(x)xy^{p^k}).$$

PROOF. This is an immediate consequence of Proposition 7.1.1 and Lemma 7.1.2 above and the fact that S_n is homogeneous of degree p^n. $\square$

7.1.1.2. *The homomorphism* ε_α. We briefly recall the definition of the homomorphism ε_α. Suppose l is a finite field of characteristic p and L is the field of fractions of the ring of Witt vectors $W(l)$ of l. Let M be a subfield of $\mathbf{C}_p$ containing L and let $\alpha \in M$ be such that $|\alpha| < 1$. We define a map

$$\begin{aligned} \varepsilon_\alpha : l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p &\to \mathcal{O}_M^\times \otimes_{\mathbf{Z}} \overline{\mathbf{F}}_p \\ a \otimes b &\mapsto E([a]\alpha) \otimes b, \end{aligned} \tag{7.1.1}$$

where $[a]$ is a Teichmüller lift of $a \in l$. It follows from [DDR16, Lem. 4.1] that this map is a homomorphism which relates the additive structure of l to the multiplicative structure of $\mathcal{O}_M^\times \otimes \mathbf{F}_p$.

LEMMA 7.1.4. *For α and ε_α as above, we have*

$$\varepsilon_{\alpha^p} \circ \mathrm{Frob} = \varepsilon_{-p\alpha},$$

where Frob *is the automorphism of* $l \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p$ *induced by the absolute Frobenius on* l.

PROOF. This is Lemma 4.3 of [DDR16, p. 14] (where we do not need the stronger hypothesis on $|\alpha|$ since we are assuming $p > 2$). □

For the last lemma of this section we will restrict ourselves to the situation that we are most interested in for this chapter. Let K be a finite extension of $\mathbf{Q}_p$ with uniformiser π_K and let L be an unramified extension of K with residue field l. Let M be a totally ramified extension of L of degree e_M and with uniformiser π such that $\pi^{e_M} \in K^\times$. As usual, let $U_i := 1 + \pi^i \mathcal{O}_M$ denote the higher unit groups in $\mathcal{O}_M^\times$.

LEMMA 7.1.5. *Suppose $\beta \in \mathcal{O}_K^\times$. Then there exist $b_{i,j}^\beta \in l$ for $i \geqslant 0$ and $j > 0$ (where the superscript emphasises the dependence on β) such that for any $m > 0$ and any $a \in l$ we have*

$$E(\beta[a]\pi^m) = E([\overline{\beta}][a]\pi^m) \prod_{\substack{i \geqslant 0 \\ j > 0}} E([b_{i,j}^\beta][a^{p^i}]\pi^{p^i m + j e_M}).$$

PROOF. We note that $\beta = (1 + \beta_0 \pi_K^{k_0})[\overline{\beta}]$ for some $k_0 \geqslant 1$ and $\beta_0 \in \mathcal{O}_K^\times$. Thus, it follows from Corollary 7.1.3 and the observation $\pi_K^{k_0} = \delta' \pi^{k_0 e_M}$ for some $\delta' \in \mathcal{O}_K^\times$ that

$$\begin{aligned} E(\beta[a]\pi^m) &= E((1 + \beta_0 \pi_K^{k_0})[\overline{\beta}][a]\pi^m) \\ &= E([\overline{\beta}][a]\pi^m) \prod_{i \geqslant 0} E(\delta_i [a^{p^i}] \pi^{p^i m + k_0 e_M}) \end{aligned} \tag{7.1.2}$$

for some $\delta_i \in \mathcal{O}_K^\times$ for $i \geqslant 0$, which depend on β only. In particular, it follows that for any $\beta \in \mathcal{O}_K^\times$, $m > 0$ and $a \in l$ we have that

$$E(\beta[a]\pi^m) \equiv E([\overline{\beta}][a]\pi^m) \bmod U_{m+1}.$$

Suppose, then, inductively that for some positive integer k and for any $\beta \in \mathcal{O}_K^\times$, $m > 0$ and $a \in l$, there exist $b_{i,j}^\beta \in l$ (depending on β only) such that

$$E(\beta[a]\pi^m) \equiv E([\overline{\beta}][a]\pi^m) \prod_{(i,j) \in I_{m,k}} E([b_{i,j}^\beta][a^{p^i}]\pi^{p^i m + j e_M}) \bmod U_{m+k},$$

where $I_{m,k} := \{(i,j) \in \mathbf{Z}_{\geqslant 0} \times \mathbf{Z}_{>0} \mid p^i m + j e_M < k\}$. The result for $E(\beta[a]\pi^m) \bmod U_{m+k+1}$ follows by applying the inductive hypothesis to the terms in equation (7.1.2) of the form $E(\delta_i[a^{p^i}]\pi^{p^i m + k_0 e_M})$. □

7.1.2. Dependence on choices. In this subsection we will give the definition of an admissible set which gives a numerical criterion on a subset of basis elements $c_{i,j}$ for their span to be independent of choices. Later we will use this criterion to find explicit formulae. This subsection is a direct generalisation of §6 of [DDR16].

Our set-up is the same as in the previous subsection. Let $p > 2$ be an odd prime. Suppose $K/\mathbf{Q}_p$ is a finite extension of ramification index e, of residue degree f and with residue field k. Moreover, we take $\chi : G_K \to \overline{\mathbf{F}}_p^\times$ to be any continuous character. Let $M = L(\pi)$ be a totally tamely ramified extension of an unramified extension L/K of degree prime-to-p, where the ramification degree e_M of M/K satisfies $e_M \mid p^f - 1$, the uniformiser π of M satisfies $\pi^{e_M} \in K^\times$ and we take M sufficiently large so that $\chi|_{G_M}$ is trivial.

7.1.2.1. *Dependencies of* (i,j). Before we can make a precise statement of the dependence of the basis on the choice of uniformiser we need to give a definition first.

Definition 7.1.6. Let f' denote the absolute niveau of χ. Recall from §5.1.2 that, for any $0 \leqslant j < e$, we have exactly f' integers $m \in \mathbf{Z}$ satisfying

(1) $\frac{jp}{p-1} < \frac{m}{p^f-1} < \frac{(j+1)p}{p-1}$,
(2) $p \nmid m$ and
(3) there exists an i such that $m \equiv n_i \bmod (p^f - 1)$.

We order these integers in some way and denote them by $m_{i',j}$ for $0 \leqslant i' < f'$.

We define the unique map $\phi_j : \{0, \ldots, f'-1\} \to \{0, \ldots, f'-1\}$ via the congruence $m_{i',j} \equiv n_{\phi_j(i')} \bmod (p^f - 1)$, or, equivalently, via the congruence $m_{i',j} \equiv n_{\phi_j(i')+kf'} \bmod (p^f-1)$ for any $k \in \{0, \ldots, f''-1\}$. If $i \in \{0, \ldots, f-1\}$, then assuming $i = i' + kf'$ (with $0 \leqslant i' < f'$ and $0 \leqslant k < f''$) we will write $\phi_j(i) := \phi_j(i') + kf'$.

Definition 7.1.7. Fix $m \in \mathbf{Z}_{>0}$. We say that $m' \in \mathbf{Z}_{>0}$ **depends on** m if there exist integers a, b and r such that

$$p^a m' = p^b m + r(p^f - 1)$$

for either

1) $a = 0$ and $(b, r) \in \mathbf{Z}_{\geqslant 0} \times \mathbf{Z}_{>0}$ or
2) $b = 0$, $a > 0$ and $r > ep\left(\frac{p^a-1}{p-1}\right)$.

DEFINITION 7.1.8. Let (i, j) and (s, t) be elements of $\mathbf{Z}/f\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z}$. We say that (s, t) depends on (i, j) if $m_{s',t}$ **depends on** $m_{i',j}$ and there exist integers a, b and r as in Definition 7.1.7 such that

a) $\phi_t(s) \equiv \phi_j(i) + b \bmod f$ if $m_{s',t} = p^b m_{i',j} + r(p^f - 1)$ or
b) $\phi_t(s) \equiv \phi_j(i) - a \bmod f$ if $p^a m_{s',t} = m_{i',j} + r(p^f - 1)$.

We note that the two conditions of Definition 7.1.7 may not be mutually exclusive, although being able to find a triple $(0, b, r)$ satisfying the first condition and a triple $(a, 0, r')$ satisfying the second condition for a fixed pair $m_{s',t}$ and $m_{i',j}$ does imply $a \equiv -b \bmod f'$. However, if $a \not\equiv -b \bmod f$ these triples will correspond to disjoint sets of dependent pairs. Similarly, it may be possible to find multiple solutions satisfying the first condition, which can lead to different dependent pairs.

Note that if $f' = f$, then the integers n_i are all distinct and we have that (s, t) depends on (i, j) if and only if $m_{s',t}$ depends on $m_{i',j}$. However, if $f' < f$, then the $m_{i',j}$ alone cannot distinguish between pairs (i, j) whose first entries lie in the same congruence class in $\mathbf{Z}/f'\mathbf{Z}$. To define dependence we must, therefore, also keep track of the index i. For a clarification of where these definitions come from, we refer the reader to the proof of Proposition 7.1.10. Note, moreover, that it follows from the bounds on the $m_{i',j}$ that the integers a, b and r in both parts of Definition 7.1.7 above can be bounded above, which leaves a finite number of checks to find all dependencies. For example, we may harmlessly suppose that $r < ep/(p-1)$ (resp. $r < ep^{a+1}/(p-1)$) in the first (resp. second) equation of Definition 7.1.7. If we suppose $p^a m' = m + r(p^f - 1)$ is a solution to the second equation, then it follows from the lower bound on r that

$$\frac{m'}{p^f - 1} > \frac{ep}{p-1}\left(1 - \frac{1}{p^a}\right).$$

Combined with $m' \leqslant \frac{ep}{p-1}(p^f - 1) - 1$ this implies that we may assume $a < \log_p\left(\frac{ep(p^f-1)}{p-1}\right)$. Similarly, it is easy to see that we may impose

$$b < \log_p\left(\frac{(e-1)p+1}{p-1}(p^f - 1)\right).$$

It follows from the bounds on the $m_{i',j}$ that $m_{s',t} > m_{i',j}$ for any (s, t) depending on (i, j). The following lemma shows that dependency is transitive, but it is clearly not symmetric or reflexive.

LEMMA 7.1.9. *Dependence is transitive.*

PROOF. We will focus on the two possibilities of Definition 7.1.7. It is easy to extend this to the full definition of Definition 7.1.8. We have four cases where in each case we suppose that m, m' and m'' are integers such that m' depends on m and m'' depends on m' in the sense of Definition 7.1.7. We need to show m'' depends on m.

Suppose that $m' = p^b m + r(p^f - 1)$ and $m'' = p^{b'} m' + r'(p^f - 1)$. Then $m'' = p^{b+b'} m + (p^{b'} r + r')(p^f - 1)$, hence it depends on m.

Suppose that $p^a m' = m + r(p^f - 1)$ (resp. $p^{a'} m'' = m' + r'(p^f - 1)$) for $r > ep\left(\frac{p^a-1}{p-1}\right)$ (resp. $r' > ep\left(\frac{p^{a'}-1}{p-1}\right)$). Then $p^{a+a'} m'' = m + (r + r' p^a)(p^f - 1)$ and

$$r + r' p^a > ep\left(\frac{p^a - 1}{p-1} + p^a \cdot \left(\frac{p^{a'} - 1}{p-1}\right)\right) = ep\left(\frac{p^{a+a'} - 1}{p-1}\right).$$

Suppose that $m' = p^b m + r(p^f - 1)$ and $p^a m'' = m' + r'(p^f - 1)$ for $r' > ep\left(\frac{p^a-1}{p-1}\right)$, so that $p^a m'' = p^b m + (r + r')(p^f - 1)$. If $b \geqslant a$, then we rewrite this as $m'' = p^{b-a} m + p^{-a}(r + r')(p^f - 1)$ and $p^{-a}(r + r') \in \mathbf{Z}_{>0}$. If $b < a$, then $p^{a-b} m'' = m + p^{-b}(r + r')(p^f - 1)$ and $p^{-b}(r + r') \in \mathbf{Z}_{>0}$. We note that $p^{-b}(r + r') > ep\left(\frac{p^{a-b} - p^{-b}}{p-1}\right) > ep\left(\frac{p^{a-b}-1}{p-1}\right)$, as required.

Lastly, we suppose that $p^a m' = m + r(p^f - 1)$ for $r > ep\left(\frac{p^a-1}{p-1}\right)$ and $m'' = p^b m' + r'(p^f - 1)$, so that $p^a m'' = p^b m + (p^b r + p^a r')(p^f - 1)$. If $b \geqslant a$, then $m'' = p^{b-a} m + (p^{b-a} r + r')(p^f - 1)$. On the other hand, if $b < a$, then $p^{a-b} m'' = m + (r + p^{a-b} r')(p^f - 1)$ and $r + p^{a-b} r' > r \geqslant ep\left(\frac{p^{a-b}-1}{p-1}\right)$, which proves the lemma. □

In the case that K is an unramified extension of $\mathbf{Q}_p$ our definition of dependency is equivalent to Definition 6.1 of [DDR16, p. 18] (although their definition is phrased in terms of the n_i instead of the $m_{i',j}$). In the case that K is a totally ramified extension of $\mathbf{Q}_p$ the definition above implies that $(0, t)$ depends on $(0, j)$ if and only if $m_{0,t} > m_{0,j}$. The last interesting special case is the **generic case**, meaning that we impose $e \leqslant a_i \leqslant p - e$ for all a_i in the tame signature of χ. Under this assumption the definition above implies that (s, t) depends on (i, j) if and only if $m_{s',t} > m_{i',j}$ and $\phi_t(s) = \phi_j(i)$. We will prove these claims later in this chapter.

Finally, recall that we had a bijection of the set of Definition 7.1.6 above with the set of integers $m' \in \mathbf{Z}$ such that

(1) $\frac{jp}{p-1} < \frac{m'}{e_M} < \frac{(j+1)p}{p-1}$,
(2) $p \nmid m'$ and
(3) there exists an i such that $m' \equiv \frac{e_M n_i}{p^f - 1} \bmod e_M$,

given by $m \mapsto m' := e_M m/(p^f - 1)$. This allowed us to rewrite the character χ as $\chi = \mu(\tau_{\phi_j(i)} \circ \overline{\omega}_\pi)^{m'_{i',j}}$ for an unramified character $\mu\colon \mathrm{Gal}(L/K) \to \overline{\mathbf{F}}_p^\times$, which is independent of i.

7.1.2.2. *Dependence on choice of uniformiser.* Recall that in Chapter 5 we defined

$$U_\chi = \left(M^\times \otimes_{\mathbf{F}_p} \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M/K)}$$

and we defined an explicit basis of this space given by $u_{i,j}$ for $0 \leqslant j < e$ and $0 \leqslant i < f$ with additionally u_{triv} (resp. u_{cyc}) if χ is trivial (resp. cyclotomic). While keeping the extension M fixed, suppose π' is a different uniformiser of M such that $(\pi')^{e_M} \in K^\times$. Using the uniformiser π' define the basis $\{u'_{i,j}\}$ and u'_{triv} if χ is trivial as in the previous section. Note that the construction of u_{cyc} is independent of the chosen uniformiser of M.

Proposition 7.1.10. *For $0 \leqslant i < f$ and $0 \leqslant j < e$, the element $u'_{i,j}$ differs from a non-zero multiple of $u_{i,j}$ by an element in the span of*

$$\{u_{s,t} \mid (s,t) \text{ depends on } (i,j)\}$$

and u_{cyc} if χ is cyclotomic.

Proof. Recall that we assume $\pi^{e_M}, (\pi')^{e_M} \in K^\times$. So if we let $\pi'/\pi = \alpha$ and $\overline{\alpha} = a \in l^\times$, then we have $\alpha^{e_M} \in K^\times$ and $a^{e_M} \in k^\times$.

Suppose first that $\alpha = [a]$, i.e. $\pi' = [a]\pi$. Then $\overline{\omega}_{\pi'} = \overline{\omega}_\pi \omega_a$, where ω_a is the unramified character of $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(l/k)$ defined on elements by $g \mapsto g(a)/a \in \mu_{e_M}(k)$. Writing, as before,

$$\chi = \mu(\tau_{\phi_j(i)} \circ \overline{\omega}_\pi)^{m'_{i',j}} = \mu'(\tau_{\phi_j(i)} \circ \overline{\omega}_{\pi'})^{m'_{i',j}},$$

we find that $\mu = \mu'(\tau_{\phi_j(i)} \circ \omega_a)^{m'_{i',j}}$. Recall that we defined $u_{i,j}$ and $u'_{i,j}$ by

$$u_{i,j} = \varepsilon_{\pi^{m'_{i',j}}}(\lambda_{\tau_{\phi_j(i)},\mu}) \text{ and } u'_{i,j} = \varepsilon_{(\pi')^{m'_{i',j}}}(\lambda_{\tau_{\phi_j(i)},\mu'}),$$

where $\lambda_{\tau_{\phi_j(i)},\mu}$ is any non-zero element of the one-dimensional μ-eigenspace $\Lambda_{\tau_{\phi_j(i)},\mu}$ of $l \otimes_{k,\tau_{\phi_j(i)}} \overline{\mathbf{F}}_p$ and similarly for $\lambda_{\tau_{\phi_j(i)},\mu'}$. If $b \in \Lambda_{\tau_{\phi_j(i)},\mu'}$, then for any $g \in \mathrm{Gal}(l/k)$ we find that

$$g((a^{m'_{i',j}} \otimes 1)b) = (g(a)^{m'_{i',j}} \otimes \mu'(g))b = (1 \otimes \mu(g))(a^{m'_{i',j}} \otimes 1)b.$$

So $(a^{m'_{i',j}} \otimes 1)\Lambda_{\tau_{\phi_j(i)},\mu'} = \Lambda_{\tau_{\phi_j(i)},\mu}$. Therefore, we are free to make the choice $\lambda_{\tau_{\phi_j(i)},\mu} = (a^{m'_{i',j}} \otimes 1)\lambda_{\tau_{\phi_j(i)},\mu'}$ and, since

$$\varepsilon_{(\pi')^{m'_{i',j}}}(\delta \otimes \gamma) = \varepsilon_{\pi^{m'_{i',j}}}(a^{m'_{i',j}}\delta \otimes \gamma),$$

we have $u_{i,j} = u'_{i,j}$ with this choice.

The preceding paragraph implies that we are free to replace π by $[a]\pi$, so we may assume without loss of generality that $\alpha \equiv 1 \bmod \pi\mathcal{O}_M$. Then $\overline{\omega}_\pi = \overline{\omega}_{\pi'}$ and hence $\mu = \mu'$. It follows that we may choose the same $\lambda_{\tau_{\phi_j(i)},\mu}$ in the definitions of $u_{i,j}$ and $u'_{i,j}$. Since $\alpha^{e_M} - 1$ is an element of $\pi\mathcal{O}_M \cap \mathcal{O}_K$, we see that $\alpha^{e_M} \equiv 1 \bmod \pi_K\mathcal{O}_K$. By Hensel's Lemma, this implies that $\alpha \in 1 + \pi_K\mathcal{O}_K$. So we can reduce to the case that $(\pi')^{m'_{i',j}} = (1+\delta\pi_K)\pi^{m'_{i',j}}$ where $\alpha^{m'_{i',j}} = 1 + \delta\pi_K$ for $\delta \in \mathcal{O}_K$.

We use Corollary 7.1.3 to obtain the formula

$$\varepsilon_{(\pi')^{m'_{i',j}}} = \varepsilon_{\pi^{m'_{i',j}}} + \sum_{k \geqslant 0} \varepsilon_{\delta_k \pi^{p^k m'_{i',j} + r_k e_M}} \circ \mathrm{Frob}^k,$$

for certain $\delta_k \in \mathcal{O}_K^\times$ and $r_k \geqslant 1$. It follows from Lemma 7.1.5 that there exist $b_{k,r} \in l$ for $k \geqslant 0$ and $r > 0$ such that

$$\varepsilon_{(\pi')^{m'_{i',j}}} = \varepsilon_{\pi^{m'_{i',j}}} + \sum_{\substack{k \geqslant 0 \\ r > 0}} \varepsilon_{[b_{k,r}]\pi^{p^k m'_{i',j} + r e_M}} \circ \mathrm{Frob}^k.$$

Hence, we obtain an equality

$$u'_{i,j} - u_{i,j} = \sum_{\substack{k \geqslant 0 \\ r > 0}} \tau_{\phi_j(i)}(b_{k,r})\varepsilon_{\pi^{p^k m'_{i',j} + r e_M}}(\mathrm{Frob}^k(\lambda_{\tau_{\phi_j(i)},\mu})).$$

If $p^k m'_{i',j} + r e_M \geqslant e p e_M/(p-1)$, then we see that the element appearing in the sum $\varepsilon_{\pi^{p^k m'_{i',j} + r e_M}}(\mathrm{Frob}^k(\lambda_{\tau_{\phi_j(i)},\mu}))$ lies in $\mathrm{Fil}^{e p e_M/(p-1)} U_\chi$, which is one-dimensional and spanned by u_{cyc} if χ is cyclotomic and zero-dimensional otherwise. Therefore, we may assume $p^k m'_{i',j} + r e_M < e p e_M/(p-1)$ and, in particular, that $r < ep/(p-1)$.

Before we continue with the proof, we prove the following claim.

Claim. For any $a > 0$ and any $r > ep\left(\frac{p^a - 1}{p-1}\right)$ such that $p^a \mid m'_{i',j} + r e_M$ we have that

$$\varepsilon_{\pi^{p^{-a}(m'_{i',j} + r e_M)}}(\mathrm{Frob}^{-a}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

lies in the span of $\{u_{s,t} \mid (s,t) \text{ depends on } (i,j)\}$ and u_{cyc} if χ is cyclotomic.

We use downwards induction on the divisibility by powers of p. Let $a \geqslant \log_p\left(\frac{e p e_M}{p-1}\right)$. Then for any $r > ep\left(\frac{p^a - 1}{p-1}\right)$ such that $p^a \mid m'_{i',j} + r e_M$ we have that

$$p^{-a}(m'_{i',j} + r e_M) > \frac{e p e_M}{p-1} - 1.$$

Since we proved that the jumps in the filtration on U_χ occur at integers, we conclude that

$$\varepsilon_{\pi^{p^{-a}(m'_{i',j} + r e_M)}}(\mathrm{Frob}^{-a}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

must be an element of $\mathrm{Fil}^{epe_M/(p-1)}U_\chi$, which gives the base case for the induction.

Fix some $k > 0$ and suppose inductively that for all $r > ep\left(\frac{p^{k+1}-1}{p-1}\right)$ such that $p^{k+1} \mid m'_{i',j} + re_M$ we have that

$$\varepsilon_{\pi^{p^{-k-1}(m'_{i',j}+re_M)}}(\mathrm{Frob}^{-k-1}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

lies in the span of $\{u_{s,t} \mid (s,t) \text{ depends on } (i,j)\}$ and u_{cyc} if χ is cyclotomic.

Now suppose that $r' > ep\left(\frac{p^k-1}{p-1}\right)$ is such that $p^k \mid m'_{i',j} + r'e_M$. We need to show that

$$\varepsilon_{\pi^{p^{-k}(m'_{i',j}+r'e_M)}}(\mathrm{Frob}^{-k}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

also lies in the required span. As before, we are free to assume that $p^{-k}(m'_{i',j} + r'e_M) < epe_M/(p-1)$, since the result is trivially true otherwise.

If $p \nmid p^{-k}(m'_{i',j} + r'e_M)$, then it follows from

$$p^{-k}(m_{i',j} + r'(p^f - 1)) \equiv n_{\phi_j(i)-k} \bmod p^f - 1$$

that $p^{-k}(m_{i',j} + r'(p^f - 1)) = m_{s',t}$ for some (s,t) depending on (i,j). Since Frob^{-k} sends $\Lambda_{\tau_{\phi_j(i)},\mu}$ to $\Lambda_{\tau_{\phi_j(i)-k},\mu}$, we conclude that

$$\varepsilon_{\pi^{p^{-k}(m'_{i',j}+r'e_M)}}(\mathrm{Frob}^{-k}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

is a multiple of $u_{s,t}$.

If $p \mid p^{-k}(m'_{i',j}+r'e_M)$, then we apply Lemma 7.1.4. Writing $-p = \beta\pi^{ee_M}$ for $\beta \in \mathcal{O}_K^\times$, we find that $\varepsilon_{\pi^{p^{-k}(m'_{i',j}+r'e_M)}}(\mathrm{Frob}^{-k}(\lambda_{\tau_{\phi_j(i)},\mu}))$ equals

$$\varepsilon_{\beta\pi^{p^{-k-1}(m'_{i',j}+(r'+p^{k+1}e)e_M)}}(\mathrm{Frob}^{-k-1}(\lambda_{\tau_{\phi_j(i)},\mu})).$$

An application of Lemma 7.1.5 shows that this lies in the span of elements of the form

$$\varepsilon_{\pi^{p^{v-k-1}(m'_{i',j}+(r'+p^{k+1}e)e_M)+we_M}}(\mathrm{Frob}^{v-k-1}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

for $v \geqslant 0$ and $w \geqslant 0$. It is easily seen that $p^{v-k-1}(r' + p^{k+1}e)e_M > \frac{epe_M}{p-1}$ if $v > 0$, so we may reduce to $v = 0$. Indeed, in the case that $v = 0$ we note that $(r' + p^{k+1}e) > ep\left(\frac{p^{k+1}-1}{p-1}\right)$, so the result follows from the inductive hypothesis. This completes the proof of the claim.

To prove the proposition, we need to show that for any $k \geqslant 0$ and $r > 0$ we have that

$$\varepsilon_{\pi^{p^k m'_{i',j}+re_M}}(\mathrm{Frob}^k(\lambda_{\tau_{\phi_j(i)},\mu}))$$

lies in the span of $\{u_{s,t} \mid (s,t) \text{ depends on } (i,j)\}$ and u_{cyc} if χ is cyclotomic. We use downward induction on the size of r (as noted above it is trivially true for $r \geqslant \frac{ep}{p-1}$).

Case 1: $p \nmid p^k m'_{i',j} + re_M$. Then, by definition, it follows from

$$p^k m_{i',j} + r(p^f - 1) \equiv n_{\phi_j(i)+k} \bmod (p^f - 1)$$

that $p^k m'_{i',j} + re_M = m'_{s',t}$ for some (s,t) which depends on (i,j). We notice, moreover, that Frob^k sends $\Lambda_{\tau_{\phi_j(i)},\mu}$ to $\Lambda_{\tau_{\phi_j(i)+k},\mu}$. We conclude that $\varepsilon_{\pi^{p^k m'_{i',j}+re_M}}(\mathrm{Frob}^k(\lambda_{\tau_{\phi_j(i)},\mu}))$ is a multiple of $u_{s,t}$.

Case 2: $p \mid p^k m'_{i',j} + re_M$ and $k > 0$. Then $r \equiv 0 \bmod p$. Letting $-p = \beta\pi^{ee_M}$ for $\beta \in \mathcal{O}_K^\times$, we use Lemma 7.1.4 to write

$$\varepsilon_{\pi^{p^k m'_{i',j}+re_M}}(\mathrm{Frob}^k(\lambda_{\tau_{\phi_j(i)},\mu})) = \varepsilon_{\beta\pi^{p^{k-1}m'_{i',j}+(\frac{r}{p}+e)e_M}}(\mathrm{Frob}^{k-1}(\lambda_{\tau_{\phi_j(i)},\mu})).$$

An application of Lemma 7.1.5 shows that this lies in the span of elements of the form

$$\varepsilon_{\pi^{p^{v+k-1}m'_{i',j}+(\frac{r}{p}+e+w)e_M}}(\mathrm{Frob}^{v+k-1}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

for $v \geqslant 0$ and $w \geqslant 0$. Note that $r < ep/(p-1)$ implies that $\frac{r}{p} + e > r$, so the result follows from the inductive hypothesis.

Case 3: $k = 0$ and $p \mid m'_{i',j} + re_M$. Again, Lemma 7.1.4 and $-p = \beta\pi^{ee_M}$ allow us to write

$$\varepsilon_{\pi^{m'_{i',j}+re_M}}(\lambda_{\tau_{\phi_j(i)},\mu}) = \varepsilon_{\beta\pi^{p^{-1}(m'_{i',j}+(r+pe)e_M)}}(\mathrm{Frob}^{-1}(\lambda_{\tau_{\phi_j(i)},\mu})).$$

Lemma 7.1.5 shows that this lies in the span of elements of the form

$$\varepsilon_{\pi^{p^{v-1}(m'_{i',j}+(r+pe)e_M)+we_M}}(\mathrm{Frob}^{v-1}(\lambda_{\tau_{\phi_j(i)},\mu}))$$

for $v \geqslant 0$ and $w \geqslant 0$. If $v - 1 \geqslant 0$, the result follows from the inductive hypothesis. If $v = 0$, the result follows from the claim above with $a = 1$. Note that the claim applies since $r + p(e+w) > ep$ and

$$p \mid m'_{i',j} + (r + p(e+w))e_M.$$

□

7.1.2.3. *Dependence on the choice of extension.* As before, suppose that $M := L(\pi)$ is a totally tamely ramified extension of L of degree e_M and with uniformiser π, where L is an unramified extension of K of degree prime to p, such that $e_M \mid p^f - 1$ and $\pi^{e_M} \in K^\times$. Recall that using the isomorphisms of local class field theory we established an isomorphism

$$\mathrm{Hom}_{\overline{\mathbf{F}}_p}\left(\left(M^\times \otimes \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M/K)}, \overline{\mathbf{F}}_p\right) \cong H^1(G_K, \overline{\mathbf{F}}_p(\chi)),$$

which naturally allows us to regard

$$U_\chi := \left(M^\times \otimes \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M/K)}$$

as the $\overline{\mathbf{F}}_p$-dual of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. We defined the basis $c_{i,j}$ for $0 \leqslant j < e$ and $0 \leqslant i < f$ together with c_{ur} and c_{tr} if χ is trivial or cyclotomic, respectively, as the dual basis to the basis of U_χ, which we denoted by $u_{i,j}$ for $0 \leqslant j < e$ and $0 \leqslant i < f$ with, possibly, u_{triv} or u_{cyc}.

Now we ask how the basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ changes if we were to use another extension $M' = L'(\pi')$ of the required form. We will denote the basis of $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ obtained via M' and π' as $c'_{i,j}$ and c'_{tr}. If χ is trivial, the basis element c_{ur} spans the one-dimensional subspace $\mathrm{Fil}^0 H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ and it is therefore well defined up to scalar regardless of the extension used in its definition. Recall from Definition 6.3.7 (cf. Definition 6.1.1) that the class c_{tr} will only be included in our exceptional subspaces when dealing with the entire space $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$. Therefore, the subspaces including this class will always be independent of the choices.

Proposition 7.1.11. *For any $0 \leqslant i < f$ and $0 \leqslant j < e$, the basis element $c'_{i,j}$ differs from a non-zero multiple of $c_{i,j}$ by an element in the span of*

$$\{c_{s,t} \mid (i,j) \text{ depends on } (s,t)\}$$

and c_{ur} if χ is trivial.

Proof. First assume we used the same extension M with different uniformisers π and π' for the definitions of the basis elements. If χ is not cyclotomic, it follows from Proposition 7.1.10 (with the roles of $u_{i,j}$ and $u'_{i,j}$ swapped) that

$$u_{i,j} = \sum_{(r,s)=(0,0)}^{(e-1,f-1)} t_{(i,j),(r,s)} u'_{(r,s)}$$

for $(t_{(i,j),(r,s)}) \in \mathrm{GL}_{ef}(\overline{\mathbf{F}}_p)$ satisfying $t_{(i,j),(i,j)} \neq 0$ and $t_{(i,j),(r,s)} = 0$ unless $(r,s) = (i,j)$ or (r,s) depends on (i,j). The dual basis then satisfies $c'_{i,j} = \sum_{(r,s)=(0,0)}^{(e-1,f-1)} t_{(r,s),(i,j)} c_{(r,s)}$ with an additional c_{un} term if χ is trivial. Thus the proposition follows for this case. If χ is cyclotomic, we noted before that u_{cyc} does not depend on the chosen uniformiser and the result follows similarly.

Now we go back to the general case. Suppose $M = L(\pi)$ and $M' = L'(\pi')$ are extensions of the required form. We claim that it suffices to prove the proposition in the special case that $L \subset L'$, $(\pi')^d = \pi$ and $de_M \mid p^f - 1$ (where e_M is the ramification degree of M over K). Indeed, if the proposition is true in these cases and M and M' are arbitrary then it follows that we may freely enlarge M and M' until $L = L'$ and π (resp. π') is a uniformiser of M (resp. M') such that $\pi^{p^f-1} \in K^\times$ (resp. $(\pi')^{p^f-1} \in K^\times$). Then, however, it follows from the fact that the ramification index of the compositum MM' over K is equal to the least common multiple of the ramification indices of M and M' over K (see, for example, [CH18, Thm. 2.1]) that $M = MM' = M'$. So π and π' are uniformisers of the same extension and the result follows from the first part of the proof. Therefore, let us now assume that $M = L(\pi)$ and $M' = L'(\pi')$, where $L \subset L'$, $(\pi')^d = \pi$ and $de_M \mid p^f - 1$. By the first part of the proof we may assume that the basis $c'_{i,j}$ (and c'_{tr} if χ is cyclotomic) is defined with respect to the special uniformiser π' of M'.

The norm map $N_{M'/M} : (M')^\times \to M^\times$ induces an isomorphism

$$\nu_{M'/M} : U'_\chi := \left((M')^\times \otimes \overline{\mathbf{F}}_p(\chi^{-1})\right)^{\mathrm{Gal}(M'/K)} \longrightarrow U_\chi.$$

We used local class field theory to identify $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ with the $\overline{\mathbf{F}}_p$-dual of both U_χ and U'_χ. Since the inclusion of absolute Galois groups $G_{M'} \hookrightarrow G_M$ under the isomorphisms of local class field theory corresponds to the norm map $N_{M'/M}$, this identification factors through the isomorphism $\nu_{M'/M}$. Therefore, it suffices to prove $\nu_{M'/M}(u'_{i,j}) = u_{i,j}$ and $\nu_{M'/M}(u'_{\mathrm{cyc}}) = u_{\mathrm{cyc}}$.

Note that the exponent of π appearing in the definition of $u_{i,j}$ is of the form $m := \frac{e_M m_{i',j}}{p^f-1}$ whereas the exponent of π' appearing in the definition of $u'_{i,j}$ is of the form $m' := \frac{de_M m_{i',j}}{p^f-1}$. Since $(\pi')^d = \pi$, it follows easily that $(\pi')^{m'} = \pi^m$ and, therefore, ε_{π^m} is equal to the restriction of $\varepsilon_{(\pi')^{m'}}$ to $l \otimes \overline{\mathbf{F}}_p$.

The embedding $\tau := \tau_{\phi_j(i)}$ used in the definition of $u_{i,j}$ and $u'_{i,j}$ is the same. Moreover, the unramified character $\mu' : \mathrm{Gal}(L'/K) \to \overline{\mathbf{F}}_p^\times$ appearing for M' is trivial on the subgroup $\mathrm{Gal}(L'/L)$ since μ is trivial on G_L. The character it induces on the quotient is simply the character $\mu : \mathrm{Gal}(L/K) \to \overline{\mathbf{F}}_p^\times$ appearing for M. The element $\lambda_{\tau,\mu'}$ lies in the μ'-eigenspace for the action of $\mathrm{Gal}(l'/k)$ on $l' \otimes_{k,\tau} \overline{\mathbf{F}}_p$. We claim that $\mathrm{tr}_{l'/l}(\lambda_{\tau,\mu'}) \in \Lambda_{\tau,\mu}$. This follows quite easily since $\mathrm{Gal}(l/k)$ acts as μ on $\Lambda_{\tau,\mu'}$. Therefore, any linear $\mathrm{Gal}(l/k)$-equivariant map $\Lambda_{\tau,\mu'} \to l \otimes_{k,\tau} \overline{\mathbf{F}}_p$ lands inside $\Lambda_{\tau,\mu}$, in particular $\mathrm{tr}_{l'/l}(\lambda_{\tau,\mu'}) \in \Lambda_{\tau,\mu}$.

From

$$\begin{aligned}
\nu_{M'/M}\varepsilon_{(\pi')^{m'}}(a \otimes 1) &= \prod_{g \in \mathrm{Gal}(M'/M)} g\varepsilon_{\pi^m}(a \otimes 1) \\
&= E\left(\sum_{g \in \mathrm{Gal}(M'/M)} g([a])\pi^m\right) \otimes 1
\end{aligned}$$

and

$$E\left(\sum_{g\in\mathrm{Gal}(M'/M)} g([a])\pi^m\right)\otimes 1 = d\varepsilon_{\pi^m}(\mathrm{tr}_{l'/l}(a)\otimes 1),$$

after extending scalars, we see that $\nu_{M'/M}(u'_{i,j}) = d\varepsilon_{\pi^m}(\mathrm{tr}_{l'/l}(\lambda_{\tau,\mu'}))$. Thus $\nu_{M'/M}(u'_{i,j})$ must be a multiple of $u_{i,j}$ as required.

The argument for u'_{cyc} follows easily from the definitions by noting that

$$N_{M'/M} : U'_{\frac{epe_M d}{p-1}} \longrightarrow U_{\frac{epe_M}{p-1}},$$

where we write U'_i for the higher unit groups in $\mathcal{O}_{M'}^\times$. $\square$

7.1.2.4. *Admissible sets.*

Definition 7.1.12. We say that a subset $J \subset \mathbf{Z}/f\mathbf{Z}\times\mathbf{Z}/e\mathbf{Z}$ is **admissible** if for any element $(s,t)\in J$ we have that $(i,j)\in J$ for any (i,j) such that (s,t) depends on (i,j). We say a subset of embeddings $J \subset \mathrm{Hom}(K,\overline{\mathbf{Q}}_p)$ is **admissible** if the corresponding subset of $\mathbf{Z}/f\mathbf{Z}\times\mathbf{Z}/e\mathbf{Z}$ is admissible.

As an immediate corollary to Proposition 7.1.11 we obtain the following result.

Corollary 7.1.13. *If $J \subset \mathrm{Hom}(K,\overline{\mathbf{Q}}_p)$ is admissible, then the image of the span of the set $\{c_\tau \mid \tau\in J\}$ in $H^1(G_K,\overline{\mathbf{F}}_p(\chi))/\mathrm{Fil}^0H^1(G_K,\overline{\mathbf{F}}_p(\chi))$ is independent of the choice of M and π.*

7.1.2.5. *Dependency graph.* Sometimes it can be helpful to draw a graph of dependencies. In such a directed graphs the vertices represent the basis elements $\{c_{i,j} \mid 0\leqslant i<f,\ 0\leqslant j<e\}$. We draw a directed line from $c_{s,t}$ to $c_{i,j}$ if (s,t) depends on (i,j) in the sense of Definition 7.1.8. We will call such a graph the **dependency graph** of the character χ. It follows from the definition that any subset of vertices forms an admissible set if all the edges going out (respecting the direction) from an element of this subset point to other elements of the subset (and not to an element outside the subset). These pictures therefore make it easy to check whether a set is admissible as well as making it easier to remember the pattern of the dependencies for different characters χ.

Figure 7.1.1 gives an example of a dependency graph.

7.2. The unramified case (d'après Dembélé–Diamond–Roberts)

In this section we will recall the explicit definition of the spaces L_V^{AH} from [DDR16]. First we recall the concepts of dependent pair and admissible set

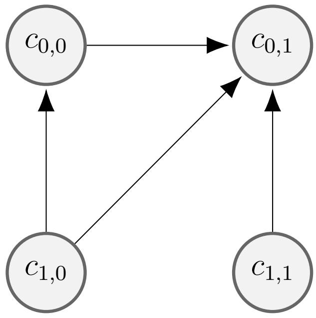

FIGURE 7.1.1. The dependency graph for $e, f = 2$ and some character χ such that the dependencies are given by: $(1,0)$ depends on $(0,0)$ and $\{(0,0),(1,0),(1,1)\}$ depend on $(0,1)$ with no further dependencies. We will see in §7.5 that, given a certain natural choice of basis elements $c_{i,j}$, this picture corresponds to the dependencies for χ when χ has tame character (a_0, p) for $1 < a_0 < p-1$.

and we show they are equivalent to our definitions under the assumption that K is an unramified extension of $\mathbf{Q}_p$. Then we recall the explicit formula given in [DDR16] for the definition of the distinguished subspaces L_V^{AH}. Lastly, we show that the explicit formula of [DDR16] in the unramified case is equivalent to our definition of the spaces L_V^{AH} – this essentially comes down to a combinatorial proof referenced from [CEGM17]. None of the results in this section are originally due to the author; the only novelty in this section is fitting these known results into the framework of this thesis.

Throughout this section we will assume K is an unramified extension of $\mathbf{Q}_p$ of residue degree f. We fix a character $\chi : G_K \to \overline{\mathbf{F}}_p^\times$ and we write

$$\chi|_{I_K} = \prod_{i=0}^{f-1} \omega_i^{a_i}$$

for integers $a_i \in [1,p]$ and $a_i < p$ for at least one i, so that $(a_0, \ldots, a_{f-1})$ denotes its tame signature. Let $M := L(\pi)$ be a totally ramified extension of K with π a distinguished uniformiser such that $\pi^{p^f-1} = -p$ and with L an unramified extension of K of prime-to-p degree sufficiently large that $\chi|_{G_M}$ is trivial. This choice of M is slightly more restrictive than the choices allowed in [DDR16]. However, there it is proved that the span L_V^{AH} is independent of the choice of the extension M and this choice will simplify our treatment.

7.2.1. Fixing basis elements. Recall that we defined the integers $m_{i',j}$ (which were used in the definitions of the basis elements $u_{i,j}$) abstractly, but never explicitly. The first task at hand will be to give an explicit definition of these integers under the assumption that K is unramified.

The integers $m_{i',0}$ were defined by imposing some ordering on the set of integers $m \in \mathbf{Z}$ satisfying

(1) $0 < \frac{m}{p^f-1} < \frac{p}{p-1}$,
(2) $p \nmid m$ and
(3) there exists an i such that $m \equiv n_i \bmod (p^f - 1)$.

Recall that this is a set of size f', where f' is the absolute niveau of the character χ. It follows fairly easily from Proposition 5.1.3 that we may give the following explicit definition of the integers $m_{i',0}$. Following [DDR16], we harmlessly extend indices from $i' \in \mathbf{Z}/f'\mathbf{Z}$ to $i \in \mathbf{Z}/f\mathbf{Z}$, which means we define $m_{i,0} := m_{i',0}$ whenever $i \equiv i' \bmod f'$. As usual, we consider indices to lie in $\mathbf{Z}$ in the obvious way when necessary, for example when we write 'the largest index smaller than i such that ...'.

Definition 7.2.1. Fix an integer $0 \leqslant i < f$. We define the integers $m_{i,0}$ explicitly in the following way.

(1) If $a_i \neq p$, then we define $m_{i,0} := n_i$.
(2) If $a_i = p$, then let j be the largest integer smaller than i such that $a_j \neq p - 1$. We define $m_{i,0} := n_j - (p^f - 1)$.

Clearly, the corresponding map $\phi_0 \colon \{0, \ldots, f-1\} \to \{0, \ldots, f-1\}$ as defined in §5.2.3 is given by

$$\phi_0(i) := \begin{cases} i & \text{if } a_i \neq p; \\ j & \text{if } a_i = p. \end{cases}$$

It is clear that we can use these integers to define the basis elements $u_{i,0}$ by the usual formula

$$u_{i,0} := \varepsilon_{\pi^{m_{i,0}}}(\lambda_{\tau_{\phi_0(i)},\mu})$$

and, dually, we also get the basis elements $c_{i,0}$.

We remark that our definition of the integers differs slightly from the definition of the analogues "n_i'" given in §5.1 of [DDR16, p. 15] for two reasons. Firstly, because of our conventions we need j to be the 'largest integer smaller than i', rather than the 'least integer greater than' as is given there (cf. §5.1). The second reason is more subtle. In the definition of [DDR16] there is an in-built shift, which would associate to i the integer $m_{i-1,0}$ under our conventions. This shift, indeed, needs to be applied to every one of the basis elements in the case that K is unramified. Since the shift function is not necessarily applied to every basis element anymore when $e > 1$, we cannot build the shift into the definition in these cases. Therefore, we believe it to be more natural for K unramified as well to apply this shift later as a part of a shift function rather than building it into the definition.

7.2.2. Dependent pairs. We now recall the definition of dependent pair from [DDR16] of which our Definition 7.1.8 is a generalisation. We will use this to give the definition of an admissible subset in the unramified case.

DEFINITION 7.2.2. ([DDR16, Defn. 6.1]) For $i, t \in \mathbf{Z}$ with $1 \leqslant t \leqslant f-1$, we say that $(i, i-t) \in (\mathbf{Z}/f\mathbf{Z})^2$ is a **dependent pair** if $a_i = p, a_{i-t} \neq p$, and

$$a_{i-1} = \cdots = a_{i-s} = p-1, \qquad a_{i-s-1} = \cdots = a_{i-t+1} = p,$$

for some $s \in 0, \ldots, t-1$.

We note that the first (resp. the second) chain of equalities is vacuous if $s = 0$ (resp. $s = t-1$). It follows from the definition that there are no dependent pairs of the form $(i, i-j)$ if $a_i \neq p$. If $a_i = p$, then there are $s+1$ dependent pairs $(i, i-j)$ for $0 < j < f$ unless

$$(a_{i-1}, \ldots, a_{i-s}, a_{i-s-1}, a_{i-s-2}, \ldots, a_i) = (p-1, \ldots, p-1, p, p, \ldots, p),$$

in which case there are s dependent pairs.

PROPOSITION 7.2.3. *For $i, t \in \mathbf{Z}$ with $1 \leqslant t \leqslant f-1$, we have that $(i, i-t) \in (\mathbf{Z}/f\mathbf{Z})^2$ is a dependent pair in the sense of Definition 7.2.2 if and only if $(i-t, 0)$ depends on $(i, 0)$ in the sense of Definition 7.1.8.*

PROOF. For simplicity we will assume $f' = f$. The case $f' < f$ follows from this fairly straightforwardly. We fix $i \in 0, \ldots, f-1$.

Firstly, suppose that $a_i \neq p$. We need to show that there exists no $(j, 0)$ such that $(j, 0)$ depends on $(i, 0)$ under Definition 7.1.8. Since we are assuming that $f = f'$ it suffices to check that there are no solutions $m' = m_{j,0}$ to the two equations of Definition 7.1.7 with $m = m_{i,0}$. We have $m = m_{i,0} = n_i \geqslant \frac{p^f-1}{p-1}$. Suppose that $m' = p^b m + r(p^f-1)$ for some $b \geqslant 0$, $r > 0$ and $m' = m_{j,0}$. Then

$$m' \geqslant \frac{p^f-1}{p-1} + (p^f-1) = \frac{p(p^f-1)}{p-1}$$

contradicting $m' < \frac{p(p^f-1)}{p-1}$. On the other hand, suppose that we have that $p^a m' = m + r(p^f-1)$ for some $a > 0$, $r > p\left(\frac{p^a-1}{p-1}\right)$ and $m' = m_{j,0}$. Then

$$\begin{aligned} r = \frac{p^a m' - m}{p^f-1} &< \frac{p^{a+1}}{p-1} - \frac{1}{p-1} \\ &= p^a + p^{a-1} + \cdots + p + 1 \end{aligned}$$

contradicting $r > p\left(\frac{p^a-1}{p-1}\right)$. So if $a_i \neq p$, then there are no $(j,0)$ such that $(j,0)$ depends on $(i,0)$, as required.

Suppose that $a_i = p$. We let $s \in 0,\dots,f-1$ be such that

$$a_{i-1} = a_{i-2} = \cdots = a_{i-s} = p-1$$

and let $t \in s+1,\dots,f-1$ be such that

$$a_{i-s-1} = a_{i-s-2} = \cdots = a_{i-t+1} = p$$

and $a_{i-t} \neq p$ if it exists. We need to show that $(i-j,0)$ depends on $(i,0)$ for $j \in 1,\dots,s-1$ and also for $j = t$ if t exists. Moreover, we need to show that there are no further dependencies under Definition 7.1.8. Since $m_{i,0} = n_{i-s-1} - (p^f-1)$, it is not hard to check that for $b = 0,\dots,s$ we have $p^b m_{i,0} = n_{i-s-1+b} - (p^f-1)$. As also

$$\begin{aligned} p^{s+1}(n_{i-s-1} - (p^f-1)) &= p(n_{i-1} - (p^f-1)) \\ &\geqslant p^{f-1} + \cdots + 2p \\ &> \frac{p^f-1}{p-1}, \end{aligned}$$

we see that the only possible solutions $m' = m_{j,0}$ to $m' = p^b m_{i,0} + r(p^f-1)$ for $b \geqslant 0$ and $r > 0$ are: $0 < b \leqslant s$, $r = 1$, $m' = m_{i-s-1+b,0} = n_{i-s-1+b}$ and $b = 0$, $r = 1$, $m' = m_{i-s-1} = n_{i-s-1}$ if $a_{i-s-1} \neq p$.

If $a_{i-s-1} \neq p$, we have found all $s+1$ dependent pairs of Definition 7.2.2. Suppose that $a_{i-s-1} = p$. Then it is easily checked that

$$n_{i-s-2} = \frac{n_{i-s-1}}{p} + (p^f-1).$$

Inserting this into the equation $n_{i-s-1} = m_{i,0} + (p^f-1)$, we obtain

$$pn_{i-s-2} = m_{i,0} + (p+1)(p^f-1).$$

If $a_{i-s-2} \neq p$, this gives us the last remaining dependency of Definition 7.2.2. Otherwise, we repeat the argument to get an equation of the form $p^a n_{i-s-1-a} = m_{i,0} + (p^a + p^{a-1} + \cdots + p + 1)(p^f-1)$ giving us the last remaining dependency: $m_{i-s-1-a,0} = n_{i-s-1-a}$ depends on $m_{i,0} = n_{i-s-1} + (p^f-1)$ for the smallest $0 < a < f-s-1$ such that $a_{i-s-1-a} \neq p$ (or no further dependency if no such a exists). If a exists, we have that $a = t-(s+1)$. We have now found all the dependencies of Definition 7.2.2 in terms of the equations of Definition 7.1.7.

Finally, we need to show that there are no further dependencies in the sense of Definition 7.1.8 if $a_i = p$. It follows from the above that we have already described all the solutions to the first equation of Definition 7.1.7. We need to show that the second equation does not have any solutions beyond the ones given already. We let s, t be as before. Suppose $p^a m' = m_{i,0} + r(p^f - 1)$ for some $a > 0$ and $r > p(p^a - 1)/(p-1)$. In particular, we have that $m' > (p - \frac{1}{p^{a-1}})\left(\frac{p^f-1}{p-1}\right)$. Clearly this inequality implies that $m' \geqslant (p^f - 1)/(p-1)$, so we need only consider solutions of the form $m' = n_k$ for some k. Letting $m' = n_k$ be such a solution, one sees that it follows from the inequality $n_k > (p - \frac{1}{p^{a-1}})\left(\frac{p^f-1}{p-1}\right)$ that

$$\begin{aligned} a_{k+1} &= a_{k+2} = \cdots = a_{k+a-1} = p, \\ a_{k+a} &= a_{k+a-1} = \cdots = a_{k+a+b-1} = p-1, \\ a_{k+a+b} &= p \end{aligned} \tag{7.2.1}$$

for some integer $b \in 0, \ldots, f-a$, where we further require $a > 1$ if $b = f - a$. Moreover, considering congruences modulo $(p^f - 1)$ and using $f = f'$, we note that $p^a n_k = (n_{i-s-1} - (p^f - 1)) + r(p^f - 1)$ implies that $k = i - s - 1 - a$. Now it is easily seen that, since $a_{i-s-1} \neq p - 1$ by assumption, the only way we can satisfy the conditions of Equation (7.2.1) is if $a_{i-s-1} = p$ and $a > 0$ is the smallest integer such that $a_{i-s-1-a} \neq p$. That is, $a = t - (s+1)$, as required. $\square$

Definition 7.2.4. We say that a subset $J \subset \mathbf{Z}/f\mathbf{Z}$ is **admissible** if for all dependent pairs (j, i) (in the sense of Definition 7.2.2), we have that if $i \in J$, then $j \in J$. We say that a subset of embeddings $J \subset \mathrm{Hom}(K, \overline{\mathbf{Q}}_p)$ is **admissible** if the corresponding subset of $\mathbf{Z}/f\mathbf{Z}$ is admissible.

Corollary 7.2.5. *If $J \subset \mathrm{Hom}(K, \overline{\mathbf{Q}}_p)$ is admissible, then the image of the span of the set $\{c_\tau \mid \tau \in J\}$ in $H^1(G_K, \overline{\mathbf{F}}_p(\chi))/\mathrm{Fil}^0 H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ is independent of the choice of M and π.*

Proof. This follows immediately from Corollary 7.1.13 and Proposition 7.2.3 or, alternatively, it is [DDR16, Cor. 6.5]. $\square$

7.2.2.1. *Dependency graphs.* Recall the definition of a dependency graph from §7.1.2.5. In the unramified case this means that we draw a directed line from $c_{j,0}$ to $c_{i,0}$ if (i, j) is a dependent pair in the sense of Definition 7.2.2. Figures 7.2.1, 7.2.2 and 7.2.3 give three examples of dependency graphs in the unramified case.

7.2.3. Shift functions. We will finish this section by giving an explicit formula for a spanning set of the spaces L_V^{AH} in terms of our basis elements

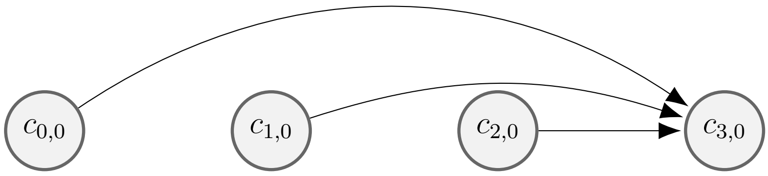

FIGURE 7.2.1. The dependency graph of a character χ with tame signature $(a_0, p-1, p-1, p)$ for any $1 \leqslant a_0 \leqslant p-2$ in the unramified case.

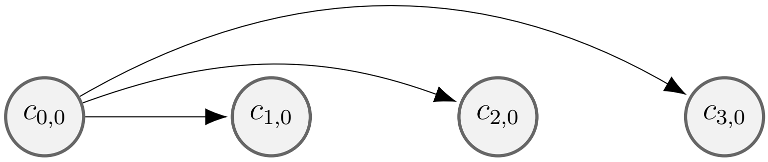

FIGURE 7.2.2. The dependency graph of a character χ with tame signature (a_0, p, p, p) for any $1 \leqslant a_0 \leqslant p-2$ in the unramified case.

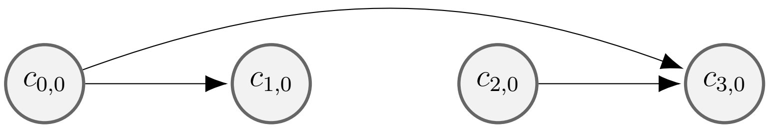

FIGURE 7.2.3. The dependency graph for a character χ with tame signature $(a_0, p, p-1, p)$ for any $1 \leqslant a_0 \leqslant p-2$ in the unramified case. This graph can be seen as a combination of the phenomena of Figure 7.2.1 and Figure 7.2.2.

$c_{i,0}$. Let us briefly recall the set-up of the beginning of Chapter 6. We assume $\rho\colon G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ is a reducible representation such that

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

for two characters $\chi_1, \chi_2\colon G_K \to \overline{\mathbf{F}}_p^\times$ and we define $\chi := \chi_1\chi_2^{-1}$. We fixed a Serre weight $V = V_{\underline{\alpha},\underline{0}}$ and we defined the integers $r_i := \alpha_i + 1 \in [1, p]$. We recall that we defined integers $s_i, t_i \in \{0\} \cup \{r_i\}$ satisfying $t_i + s_i = r_i$, which correspond to the minimal and maximal Kisin modules of [GLS15]. We note that the interval $\mathcal{I}_i = \varnothing$ if $t_i \geqslant r_i$ and $\mathcal{I}_i = \{0\}$ if $t_i < r_i$ (see Definition 6.1.3).

DEFINITION 7.2.6. We define a subset $J \subset \mathbf{Z}/f\mathbf{Z}$ via

$$J := \{i \in \mathbf{Z}/f\mathbf{Z} \mid t_i < r_i\}.$$

This subset now corresponds to the embeddings τ_i for which we see "a positive dimension at i" and plays the same role as the set J which is described in [DDR16, §2.2]. In fact, since we chose our integers s_i, t_i to correspond to the minimal and maximal Kisin modules of [GLS15], the J above is equal to $J_{\max}$ as described in [DDR16, §7.2].

7.2.3.1. *Shifting functions δ and μ.* Given any subset $J' \subset \mathbf{Z}/f\mathbf{Z}$ we would like to define a subset $\mu(J')$ of $\mathbf{Z}/f\mathbf{Z}$ which is admissible. We will follow the precise, but rather difficult to understand, definition of [DDR16, §7.1] of the shifting function μ and then write a few words on how to best interpret this definition.

First we define a function $\delta : \mathbf{Z} \to \mathbf{Z}$ depending on $(a_0, \ldots, a_{f-1})$ as follows: if $j \in \mathbf{Z}$, then we define $\delta(j) = j$ unless

$$(a_{j+1}, \ldots, a_{i-1}, a_i) = (p-1, \ldots, p-1, p)$$

for some (necessarily unique) $i > j$, in which case we define $\delta(j) = i$; we include the case $a_i = p$ and $j = i-1$ here. This induces a function $\mathbf{Z}/f\mathbf{Z} \to \mathbf{Z}/f\mathbf{Z}$ which we also denote by δ. If $\delta(J') \subset J'$, then we define $\mu(J') := J'$. Otherwise, we choose some $[i_1] \in \delta(J') \backslash J'$ and we let j_1 be the greatest integer such that $j_i < i_1$, $j_1 \in J'$ and $\delta(j_1) = i_1$. Now write $J' = \{[j_1], \ldots, [j_r]\}$ with $j_1 > j_2 > \cdots > j_r > j_1 - f$, and define i_κ for $\kappa = 2, \ldots, r$ inductively by

$$i_\kappa = \begin{cases} \delta(j_\kappa) & \text{if } i_{\kappa-1} > \delta(j_\kappa); \\ j_\kappa & \text{otherwise.} \end{cases}$$

Then we set $\mu(J') = \{[i_1], [i_2], \ldots, [i_r]\}$.

LEMMA 7.2.7. *The set $\mu(J')$ is admissible.*

PROOF. This is Lemma 7.1 [DDR16, p. 22]. $\square$

An alternative description of the shift function μ comes from [CEGM17, p. 17]:

> We define $\mu(J') = J'$, unless there is some $i \notin J'$ for which we have $a_i = p, a_{i-1} = p-1, \ldots, a_{i-s} = p-1, a_{i-s-1} \neq p-1$, and at least one of $i-1, i-2, \ldots, i-s-1$ is in J'. If this is the case, we let x be minimal such that $i - x \in J'$, and we consider the set obtained from J' by replacing $i-x$ with i. Then $\mu(J')$ is the set obtained by simultaneously making all such replacements (that is, making these replacements

for all possible i).

This definition gives a better intuition for the shift function μ, however in exceptional situations we believe that it is not always clear how one should interpret this definition. Imagine, for example, that $f = 4$, the character has tame signature $(a_0, p, p-1, p)$ for $1 \leqslant a_0 < p-1$ and $J' = \{0, 1\}$. Then $\mu(J') = \{1, 3\}$, because we should initially replace 1 by 3 and 0 by 1 after. In this example we see that it matters that the replacements are done successively rather than 'simultaneously'. Therefore, the last sentence of the definition of [CEGM17] above seems unfortunate. If this sentence were to be replaced by "Then $\mu(J')$ is the set obtained by successively making all such replacements (that is, we start with the replacement of $i-x$, then we replace $i-x-1$ if necessary (taking previous replacements into account) and we continue like this until $i-x-(f-1)$).", then we would believe the definition of [CEGM17] to be correct.

7.2.4. The spaces L_V^{AH} in the unramified case. We are almost ready to state the explicit formula of [DDR16] for the spaces L_V^{AH}. First we need to define one more simple shift function. This shift function is built into all the definitions in [DDR16]: for example, they let $u_{i,0}$ be defined using n_{i-1} if $a_{i-1} \neq p$, whereas we used n_i to define $u_{i,0}$ if $a_i \neq p$.

Definition 7.2.8. We define $\gamma : \mathbf{Z} \to \mathbf{Z}$ as mapping $i \mapsto i-1$. The induced map $\mathbf{Z}/f\mathbf{Z} \to \mathbf{Z}/f\mathbf{Z}$ will also be denoted by γ.

Recall that we defined the subsets of embeddings $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ in Definition 6.3.5, which determine which basis elements are included in $L_V^{\mathrm{AH}}(\chi_1, \chi_2)$. Let J be the set of embeddings as in Definition 7.2.6. Then we have the following proposition.

Proposition 7.2.9. *We have that*

$$J_V^{\mathrm{AH}}(\chi_1, \chi_2) = \mu(\gamma(J)).$$

Proof. It follows from the definitions and the results of Chapter 6 that these two sets have the same cardinality, therefore it suffices to prove one inclusion. We will prove: $(i, 0) \in J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ implies that $i \in \mu(\gamma(J))$.

We assume that $(i, 0) \in J_V^{\mathrm{AH}}(\chi_1, \chi_2)$. Rewriting the equations of Definition 6.3.5 to the case at hand we find that this assumption is equivalent to the following requirement: there exists $k \in J$ and $m \geqslant 0$ such that

(1) $p^m m_{i',0} = \xi_k$ and

(2) $\phi_0(i) \equiv k - m \bmod f$.

It follows from the combinatorics of §3.6 of [CEGM17] that these two equations imply that $i \in \mu(\gamma(J))$ (in particular, see Proposition 3.6.7). (Note that we need to apply the shift γ only in reference to i, since we have 'unshifted' $m_{i',0}$ and $\phi_0(i)$ compared to [CEGM17]. Our ξ_k is the same as theirs so it is not necessary to apply γ when referring to k.) $\square$

7.3. The totally ramified case

In this section we will give an explicit formula for the elements of the set $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ under the assumption that K is a totally ramified extension of $\mathbf{Q}_p$. These are results that are originally due to the author, which were collected in an early stage of the PhD as part of a statement and proof of the conjecture of [DDR16] in the totally ramified case.

In this section K is a totally ramified extension of $\mathbf{Q}_p$ of degree e, residue field $k = \mathbf{F}_p$ and with fixed uniformiser π_K. We denote the unique embedding $k \to \overline{\mathbf{F}}_p$ by τ_0. Given a continuous character $\chi : G_K \to \overline{\mathbf{F}}_p^\times$, we let $M := L(\pi)$ be a tamely ramified extension of K where π is a root of $x^{p-1} + \pi_K$ and L is an unramified extension of K of prime-to-p degree such that $\chi|_{G_M}$ is trivial. We let $1 \leqslant a_0 < p$ be the unique integer such that $\chi|_{I_K} = \omega_0^{a_0}|_{I_K}$.

7.3.1. Fixing basis elements. As before in the unramified case we need to make a 'natural' choice of the integers $m_{0,j}$ appearing in the definition of our basis elements $u_{0,j}$. However, in the totally ramified case it turns out there is really only one possibility.

Definition 7.3.1. For $0 \leqslant j < e$, we define $m_{0,j}$ to be the unique integer m such that $pj < m < p(j+1)$ and

$$m \equiv a_0 \bmod (p-1).$$

Note that the integer is unique since the interval has length $(p-1)$. We may leave the condition $p \nmid m$ from before out, since the boundaries and length of our interval ensure that p never divides m. Therefore, we could have equivalently defined $\{m_{0,0}, \ldots, m_{0,e-1}\}$ to be the set

$$\{m \in \mathbf{Z} \mid 0 < m < pe,\ p \nmid m \text{ and } m \equiv a_0 \bmod (p-1)\}$$

ordered by size. It is not hard to give a formula for the integers $m_{0,j}$.

Lemma 7.3.2. *For $0 \leqslant j < e$, write $j \equiv r \bmod (p-1)$ for $0 \leqslant r < (p-1)$. Then*

$$m_{0,j} = \begin{cases} pj + a_0 - r & \text{if } a_0 > r; \\ p(j+1) - 1 + a_0 - r & \text{if } a_0 \leqslant r. \end{cases}$$

Proof. This is easily checked from the definition. □

Specialising the methods of §5.2.3 to the case at hand, we may then define the basis elements

$$u_{0,j} := \varepsilon_{\pi^{m_{0,j}}}(\lambda_{\tau_0,\mu})$$

and we define the basis elements $c_{0,j}$ dually.

7.3.2. Explicit dependencies. Next we need to give an explicit description of the dependency criterion in the totally ramified case. We do this in the following proposition.

Proposition 7.3.3. *Fix two integers $0 \leqslant j, j' < e$. We have that $(0, j')$ depends on $(0, j)$ (in the sense of Definition 7.1.8) if and only if $j' > j$.*

Proof. Let us write $m =: m_{0,j}$. Since $f = 1$, the congruences of Definition 7.1.8 are automatically satisfied. For the second equation of Definition 7.1.7, we note that if $p^a m' = m + r(p-1)$ for $a > 0$ and $r > ep\left(\frac{p^a-1}{p-1}\right)$, then $m' > ep + p^{-a}(a_0 - 1) \geqslant ep$ contradicting the bounds on the integers $m_{0,j}$. Therefore, we only need to consider m' of the form $m' = p^b m + r(p-1)$ for $b \geqslant 0$ and $r > 0$. It is clear from the definitions that if $m' = m_{0,j'}$ for some $j' > j$, then m' is a solution to this equation for some $r > 0$ (and $b = 0$).

Conversely, suppose $m' = m_{0,j'}$ is a solution to the equation for some j'. Then $m' > m$, hence $j' > j$. □

7.3.2.1. *Dependency graph.* Recall from §7.1.2.5 the notion of a dependency graph. In the totally ramified case we get the particularly easy dependency graph of Figure 7.3.1.

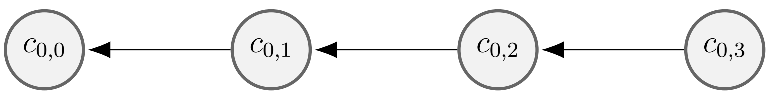

Figure 7.3.1. The dependency graph of any character χ in the totally ramified case (assuming $e = 4$).

7.3.3. The spaces L_V^{AH} in the totally ramified case. The previous subsection suggests that if d is the dimension of the space L_V, then we may be able to simply define L_V^{AH} as the span of the basis elements $c_{0,0}, \ldots, c_{0,d-1}$ – although we have to be slightly more careful if χ is trivial and/or cyclotomic. This is what we will do in this section.

We fix a reducible representation $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ of the form

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

for characters $\chi_1, \chi_2 : G_K \to \overline{\mathbf{F}}_p^\times$ and we let $\chi := \chi_1\chi_2^{-1}$. Write c_ρ for the extension class in $H^1(G_K, \overline{\mathbf{F}}_p(\chi))$ associated to ρ. We, furthermore, fix a Serre weight $V = V_{\alpha_0,0}$ and, as before, we define $r_0 := \alpha_0 + 1 \in [1, p]$.

Similarly to what we did in §6.1.2, we will exclude the exceptional case in which χ is cyclotomic, $r_0 = p$ and χ_2 is unramified. In this case $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ consists simply of all elements $(0, j)$ for $0 \leqslant j < e$, so there is nothing to prove.

We need to define integers t_0, s_0 corresponding to the minimal and maximal Kisin modules of [GLS15]. We may write $\chi_2|_{I_K} = \omega_0^{m_0}|_{I_K}$ for a unique $0 \leqslant m_0 < p - 1$.

LEMMA 7.3.4. *If $c_\rho \in L_V(\chi_1, \chi_2)$ and $\dim_{\overline{\mathbf{F}}_p} L_V(\chi_1, \chi_2) > 0$, then*

$$m_0 \in [0, e-1] \cup [r_0, r_0 + e - 1].$$

PROOF. The statement is automatic if either $e \geqslant p - 1$ or $m_0 = 0$ (i.e. χ_2 is unramified). Therefore, assume that $e \leqslant p - 2$ and $m_0 > 0$. Suppose for a contradiction that $m_0 \notin [0, e-1] \cup [r_0, r_0+e-1]$. From $c_\rho \in L_V(\chi_1, \chi_2)$ it follows (see [GLS15, §4.1.2]) that there exist pairs (J, x_0) with J a subset of $\mathrm{Hom}(k, \overline{\mathbf{F}}_p)$ (i.e. either J is empty or contains the unique embedding τ_0) and with $x_0 \in [0, e-1]$ an integer such that

$$\rho|_{I_K} \cong \begin{pmatrix} \prod_{\tau_0 \in J} \omega_0^{r_0 + x_0} \prod_{\tau_0 \notin J} \omega_0^{x_0} & * \\ 0 & \prod_{\tau_0 \in J} \omega_0^{e-1-x_0} \prod_{\tau_0 \notin J} \omega_0^{r_0+e-1-x_0} \end{pmatrix}.$$

Fix a pair (J, x_0). If $J = \{\tau_0\}$, then $m_0 = e - 1 - x_0$ contradicting the assumption that $m_0 \notin [0, e-1]$. Thus we assume $J = \varnothing$. Then

$$m_0 \equiv r_0 + (e-1) - x_0 \bmod (p-1).$$

Since $1 \leqslant r_0 + e - 1 - x_0 \leqslant 2p - 3$, either m_0 or $m_0 + (p-1)$ equals $r_0 + e - 1 - x_0$. The former contradicts $m_0 \notin [r_0, r_0 + e - 1]$, while it follows from the latter that if either $r_0 < p$ or $x_0 > 0$, then we must have $m_0 \leqslant e-1$ again contradicting our assumptions.

The last remaining case is $r_0 = p$, $J = \varnothing$ and $x_0 = 0$. Then our representation has the form

$$\rho|_{I_K} \cong \begin{pmatrix} 1 & * \\ 0 & \omega_0^e \end{pmatrix}.$$

Looking at all possible pairs (J, x_0) for this ρ, we note that if $J \neq \varnothing$, then considerations on the subspace character give $p + x_0 \equiv x_0 + 1 \equiv 0 \bmod (p-1)$. Since $x_0 \leqslant p-3$, this gives a contradiction. Again, considerations on the subspace character for $J = \varnothing$ show that $(J, x_0) = (\varnothing, 0)$ is the only possible pair for this ρ. Then it follows from [GLS12, Lem. 4.2.2] that $\dim_{\overline{\mathbf{F}}_p} L_V(\chi_1, \chi_2) = 0$. Note that we can't have $\chi_1 = \chi_2$, since we are assuming $e < p-1$. ☐

It follows from the lemma that we may define $t_0 := m_0 \in [0, p-2]$. As before, we define $s_0 := r_0 + e - 1 - t_0$ and $\xi_0 := ps_0 - t_0$. Recall the definition of the set $\mathcal{I}_0$ from Definition 6.1.3:

$$\mathcal{I}_0 := \begin{cases} [0, s_0 - 1] & \text{if } t_0 \geqslant r_0, \\ \{t_0\} \cup [r_0, s_0 - 1] & \text{if } t_0 < r_0. \end{cases}$$

Definition 7.3.5. With s_0, t_0 and $\mathcal{I}_0$ as above, we define

$$\delta_0 := |\mathcal{I}_0| = \begin{cases} s_0 & \text{if } t_0 \geqslant r_0, \\ 1 + s_0 - r_0 & \text{if } t_0 < r_0. \end{cases}$$

It follows from the dimension formulae in the proof of Theorem 5.4.1 of [GLS15] that we should think of δ_0 as roughly being equal to $\dim_{\overline{\mathbf{F}}_p} L_V(\chi_1, \chi_2)$ except for some exceptional cases in which the quotient of the two characters is trivial or cyclotomic. The explicit formula for the set $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ is given in the following proposition.

Proposition 7.3.6. *Let $0 \leqslant j < e$. Then*

$$(0, j) \in J_V^{\mathrm{AH}}(\chi_1, \chi_2) \textit{ if and only if } j < \delta_0.$$

7.3.4. Combinatorics. The goal of this subsection will be to prove Proposition 7.3.6. Unravelling definitions, we see that this proposition is equivalent to the following proposition.

Proposition 7.3.7. *Let $0 \leqslant j < e$. Then the equation*

$$p^k m_{0,j} = \xi_0 - d(p-1)$$

has a solution for some $d \in \mathcal{I}_0$ *and* $k \geqslant 0$ *if and only if* $j < \delta_0$.

We will prove this proposition through a series of lemmas and intermediate results. Let v_p denote the standard p-adic valuation on $\mathbf{Z}$. Suppose that $p^k m_{0,j} = \xi_0 - (p-1)i$ for some $i \in \mathcal{I}_0$ and $j \in [0, e-1]$. Since $p \nmid m_{0,j}$, we see that $k := v_p(\xi_0 - (p-1)i)$ is uniquely determined by s_0, t_0 and i. Moreover, $m_{0,j}$ is then also uniquely determined by this triple. We will refer to the values $\frac{\xi_0-(p-1)i}{p^k}$ for $i \in \mathcal{I}_0$ and $k = v_p(\xi_0 - (p-1)i)$ as **potential** $m_{0,j}$**-values**.

Since the p-adic valuation of the integers $\xi_0 - (p-1)i$ for $i \in \mathcal{I}_0$ is important, let us group together elements with the same valuation. For $k \geqslant 0$, let us define $S_k := \{i \in \mathcal{I}_0 \mid v_p(\xi_0 - (p-1)i) = k\}$ and let us write $S_{\geqslant k} := \bigcup_{m \geqslant k} S_m$. We make the trivial observation that $i \in S_{\geqslant 1}$ if and only if $i \equiv t_0 \bmod p$. The following lemma shows that an element of S_m for $m > k$ always leads to a strictly smaller potential $m_{0,j}$-value than an element of S_k.

Lemma 7.3.8. *Suppose* $k \geqslant 1$ *and let* i_1 *(resp.* i_2*) be an element of* S_k *(resp.* S_{k-1}*). Then*

$$\frac{\xi_0 - (p-1)i_1}{p^k} < \frac{\xi_0 - (p-1)i_2}{p^{k-1}}.$$

Proof.

$$\begin{aligned}\xi_0 - (p-1)i_1 &< p(\xi_0 - (p-1)i_2)\\ &\iff p(p-1)i_2 - (p-1)i_1 < (p-1)\xi_0\\ &\iff pi_2 - i_1 < ps_0 - t_0\\ &\iff p(i_2 - s_0) < i_1 - t_0.\end{aligned}$$

Since any $i \in \mathcal{I}_0$ satisfies $i \leqslant s_0 - 1$, we find $p(i_2 - s_0) \leqslant -p$. Whereas $i_1 - t_0 \geqslant -t_0 \geqslant -(p-2)$, so the final inequality is always satisfied. $\square$

Lemma 7.3.9. *For any* $i \in \mathcal{I}_0$*, there exists a unique* $0 \leqslant j < e$ *such that*

$$p^k m_{0,j} = \xi_0 - (p-1)i$$

for some $k \geqslant 0$*. Furthermore, if* $m_{0,j}$ *is a solution of such an equation, then it determines* i *uniquely.*

Proof. Fix some $i \in \mathcal{I}_0$ and let $k := v_p(\xi_0 - (p-1)i)$. We already noted that $m_{0,j}$, if it exists, is uniquely determined by ξ_0 and $i \in \mathcal{I}_0$. Recall, moreover, that we proved in Lemma 6.2.2 that $\xi_0 \equiv a_0 \bmod (p-1)$. Hence, also $\frac{\xi_0-(p-1)i}{p^k} \equiv a_0 \bmod (p-1)$. Therefore, by definition of the integers $m_{0,j}$, it suffices to prove $0 < \frac{\xi_0-(p-1)i}{p^k} < pe$.

The first inequality follows from

$$\begin{aligned} \xi_0-(p-1)i &\geqslant ps_0-t_0-(p-1)(s_0-1) \\ &= s_0+(p-1-t_0) > 0 \end{aligned}$$

as $t_0 \in [0, p-2]$.

For the second inequality, first assume $t_0 \geqslant r_0$. In this case, we have $\xi_0-(p-1)i \leqslant \xi_0$ and

$$\xi_0 = p(r_0+e-1)-(p+1)t_0 = p(r_0-t_0-1)+pe-t_0 < pe.$$

Assume then $t_0 < r_0$. We note that $\mathcal{I}_0 = \{t_0\} \cup [r_0, s_0-1]$ and $t_0 \in S_{\geqslant 1}$. Since $\frac{\xi_0-(p-1)t_0}{p} = s_0-t_0 < pe$ (except when $e=1, r_0=p$ and $t_0=0$), we see that by the previous lemma the potential $m_{0,j}$-value associated to any $i \in S_{\geqslant 1}$ satisfies the required inequality. (In the exceptional case $e=1, r_0=p$ and $t_0=0$, we see that the potential $m_{0,j}$-value corresponding to the unique element of $\mathcal{I}_0$ is $\frac{\xi_0-(p-1)t_0}{p^2}=1$, so we can disregard this case.) Therefore, we may restrict ourselves to considering potential $m_{0,j}$-values associated to $i \in S_0$. In particular, we may assume $i \geqslant r_0$. Again, by Lemma 7.3.8 it suffices to note

$$\xi_0-(p-1)i \leqslant ps_0-t_0-(p-1)r_0 < pe$$

unless $i=r_0=p$ and $t_0=0$ in which case $r_0 \in S_{\geqslant 1}$. In the last case, if also $s_0 > r_0+1$, then it suffices to note that $i=r_0+1$ is the smallest element of S_0 and satisfies the inequality.

The last claim follows from Lemma 7.3.8 and the easy observation that if $i_1, i_2 \in S_k$ correspond to the same $m_{0,j}$ then $i_1=i_2$. □

Proof of Proposition 7.3.7. We will write $\delta := \delta_0$. By Lemma 7.3.9, Definition 7.3.1 and as $\delta = |\mathcal{I}_0|$ by definition, it suffices to prove that the largest potential $m_{0,j}$-value occurring for $i \in \mathcal{I}_0$ lies in the interval $(p(\delta-1), p\delta)$.

Assume first that $t_0 \geqslant r_0$, so that $\mathcal{I}_0 = [0, s_0-1]$ and $\delta = s_0$. We claim that the largest potential $m_{0,j}$-value occurs in the interval $(p(s_0-1), ps_0)$ in this case. By Lemma 7.3.8 the largest potential $m_{0,j}$-value occurring for $i \in \mathcal{I}_0$ is equal to ξ_0 if $t_0 \not\equiv 0 \bmod p$ and it is equal to $\xi_0-(p-1)$ otherwise. If $t_0 \not\equiv 0 \bmod p$, then $ps_0 > \xi_0 = ps_0-t_0$ is obvious as $t_0 \neq 0$ and $ps_0-t_0 > ps_0-p$ follows since $t_0 \leqslant p-2$. We may, therefore, suppose that $t_0 \equiv 0 \bmod p$. Then $t_0=0$ as $t_0 \in [0, p-2]$. So the largest potential $m_{0,j}$-value is $\xi_0 - (p-1)$. (Note that in the special case where $s_0 = 1$ and $t_0 \equiv 0 \bmod p$, we have that the largest potential $m_{0,j}$-value is $\xi_0/p = 1$, which happens to equal $\xi_0 - (p-1)$, so we do not have to treat this case separately.) The inequalities become $ps_0 > ps_0 - (p-1)$ and $ps_0 - (p-1) > ps_0 - p$ which are both obvious.

Now assume that $t_0 < r_0$, so that $\mathcal{I}_0 = \{t_0\} \cup [r_0, s_0 - 1]$ and $\delta = s_0 - r_0 + 1$. We claim that the largest potential $m_{0,j}$-value for $i \in \mathcal{I}_0$ occurs in the interval $(p(s_0 - r_0), p(s_0 - r_0 + 1))$. By Lemma 7.3.8 the largest potential $m_{0,j}$-value must come from an $i \in S_0$ unless no such i exists. Suppose first that S_0 is non-empty. Since $t_0 \in S_{\geqslant 1}$, this means the largest potential $m_{0,j}$-value is equal to $\xi_0 - (p-1)r_0$ if $r_0 \not\equiv t_0 \bmod p$ and $\xi_0 - (p-1)(r_0+1)$ otherwise. In the former case we must prove the inequality $p(s_0 - r_0 + 1) > ps_0 - t_0 - (p-1)r_0$, which follows from $p > r_0 - t_0$ (note that this is satisfied since $r_0 = p$ and $t_0 = 0$ contradicts our assumption $r_0 \not\equiv t_0 \bmod p$), and the inequality $ps_0 - t_0 - (p-1)r_0 > ps_0 - pr_0$, which follows from the assumption that $r_0 > t_0$. In the latter case, we observe that $r_0 \equiv t_0$ and $r_0 > t_0$ together imply that $r_0 = p$ and $t_0 = 0$. We must prove the inequality $p(s_0 - p + 1) > ps_0 - (p-1)(p+1)$, which is clear, and the inequality $ps_0 - (p-1)(p+1) > ps_0 - p^2$, which is also clear.

Suppose that $t_0 < r_0$ and $S_0 = \varnothing$. We either have that $s_0 = r_0$ or that $s_0 = r_0 + 1$ and $r_0 \equiv t_0 \bmod p$. In the latter case, as we observed above, we must have $r_0 = p$ and $t_0 = 0$. We conclude that $p \nmid s_0 - t_0 = p + 1$, so the largest potential $m_{0,j}$-value is $\frac{\xi_0 - (p-1)t_0}{p} = s_0 - t_0$. The inequalities we need to prove are then $2p = p(s_0 - r_0 + 1) > s_0 - t_0 = p + 1$, which is clear, and $p + 1 > p$, also clear. Finally suppose that $s_0 = r_0$. Then the largest potential $m_{0,j}$-value is, again, $s_0 - t_0$ unless $r_0 = p$ and $t_0 = 0$ in which case it is 1. In the first case, the inequalities become $p > r_0 - t_0$, which follows since either $r_0 < p$ or $t_0 > 0$, and $r_0 - t_0 > 0$, which follows from the assumption that $t_0 < r_0$. Finally, in the second case $s_0 = r_0 = p$, $t_0 = 0$ and the largest potential $m_{0,j}$-value is 1. The inequalities are then $p > 1$ and $1 > 0$, which are trivially satisfied. This finishes the proof. $\square$

7.4. Explicit formulae in generic cases

In this section, we will make a conjecture for an explicit formula for the elements of $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ under the condition that the quotient of the characters is *generic*. All the conjectures in this chapter are backed up by ample computational evidence gathered by the author using [SageMath].

7.4.1. Genericity. Our set-up is the same as in the general case in Chapter 5. Let K be an extension of $\mathbf{Q}_p$ of ramification degree e and residue degree f. We start with a representation $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ such that

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}.$$

We write $\chi := \chi_1\chi_2^{-1}$ for the quotient and let $\chi|_{I_K} = \prod_i \omega_i^{a_i}$ for $a_i \in [1,p]$. We define

$$n_i := \sum_{j=1}^{f} a_{i+j}p^{f-j} = a_{i+1}p^{f-1} + \cdots + a_{i+f-1}p + a_i$$

and we let f' denote the absolute niveau of χ (see §5.1). We fix a uniformiser $\pi_K \in K$ and define $M := L(\pi)$ to be a totally tamely ramified extension of an unramified prime-to-p extension L of K, where the ramification degree e_M of M/K satisfies $e_M \mid p^f - 1$ and the uniformiser π of M satisfies $\pi^{e_M} \in K^\times$, and we take M sufficiently large so that $\chi|_{G_M}$ is trivial.

Definition 7.4.1. We say that the character χ (or the representation ρ) is **generic** if $e \leqslant a_i \leqslant p - e$ for all i.

In particular, genericity implies that $e \leqslant p/2$. For the remainder of the section we will assume that χ is generic. Intuitively genericity should correspond to the idea that there are no dependencies except the trivial ones, or, equivalently, to the idea that we have a direct sum decomposition of $H^1(G_K, \overline{\mathbf{F}}_p(\chi)$ which respects the filtration. We note that this definition of genericity is more general than the definition used in other sources. For example, in [DS15] they define dependency as meaning that $e \leqslant a_i \leqslant p-1-e$ for all i and §5 of their paper shows that their methods do not work for the more lenient definition above. However, in the unramified case it follows from §7.2 that $1 \leqslant a_i \leqslant p-1$ is enough to rule out any dependencies, which suggests that our definition is more natural than the one used in [DS15].

7.4.2. Explicit basis elements. As we have done in the previous sections, our first goal will be to give a natural explicit definition of the integers $m_{i',j}$ under the assumption that χ is generic. For $0 \leqslant j < e$, recall that the integers $m_{0,j}, \ldots, m_{f'-1,j}$ were defined as the integers $m \in \mathbf{Z}$ satisfying

(1) $\frac{jp}{p-1} < \frac{m}{p^f-1} < \frac{(j+1)p}{p-1}$,
(2) $p \nmid m$ and
(3) there exists an i such that $m \equiv n_i \bmod p^f - 1$.

We will now give an explicit definition.

Definition 7.4.2. For $0 \leqslant j < e$ and $0 \leqslant i' < f'$, we define

$$m_{i',j} := n_{i'} + j(p^f - 1)$$

and we accordingly define $m'_{i',j} := e_M m_{i',j}/(p^f - 1)$.

Clearly, our function ϕ_j as in §5.2 then becomes the identity map

$$\mathrm{id}\colon \{0, \dots, f' - 1\} \to \{0, \dots, f' - 1\}.$$

Lemma 7.4.3. *The integers $m_{i',j}$ satisfy the three conditions above and are all distinct.*

Proof. Distinctness is clear since $n_0, \dots, n_{f'-1}$ are distinct. Also the third condition is clear. For the first condition, we note that it follows from the genericity hypothesis that

$$\frac{e}{p-1} \leqslant \frac{n_{i'}}{p^f - 1} \leqslant \frac{p-e}{p-1}.$$

Now the condition follows from the inequalities $\frac{e}{p-1} + j > \frac{jp}{p-1} = \frac{j}{p-1} + j$, which is always satisfied since $e > j$, and $\frac{p-e}{p-1} + j = \frac{(j+1)p-(e+j)}{p-1} < \frac{(j+1)p}{p-1}$, which is satisfied as $j + e > 0$.

For the second condition, we note that $m_{i',j} = n_{i'} + j(p^f - 1)$ is congruent to $a_{i'} - j \bmod p$. Since $1 \leqslant a_{i'} - j \leqslant p - e$, we see that $m_{i',j} \not\equiv 0 \bmod p$. $\square$

We define the basis elements $u_{i,j}$ using these definitions as in §5.2. Our basis elements are defined by

$$u_{i,j} := \varepsilon_{\pi^{m'_{i',j}}}(\lambda_{\tau_i,\mu}).$$

7.4.3. Dependencies. In this subsection we prove the following proposition giving an explicit replacement of Definition 7.1.8 when we are in the generic case.

Proposition 7.4.4. *Fix integers $0 \leqslant i, s < f$ and $0 \leqslant j, t < e$. Then (s, t) depends on (i, j) (in the sense of Definition 7.1.8) if and only if $s = i$ and $t > j$.*

Proof. We note that it is clear with the explicit definitions above that $m_{i',t}$ depends on $m_{i',j}$ for any $t > j$ under the first equation of Definition 7.1.7 with $b := 0$ and $r := t - j$. It then follows from the first equation of Definition 7.1.8 that these 'dependent integers' lead to the dependent pair (i, t) depending on (i, j) if $t > j$. Note that these dependencies include all the solutions to the first equation of Definition 7.1.7 with $b = 0$.

We must show that there are no further dependencies. We first note that if $m' = p^b m_{i',j} + r(p^f - 1)$ for some $b, r > 0$, then

$$m' \geqslant pn_{i'} + r(p^f - 1) \geqslant p\left(\frac{e(p^f-1)}{p-1}\right) + (p^f - 1) > \frac{ep}{p-1}(p^f - 1).$$

Hence, the first equation of Definition 7.1.7 will never be satisfied for any $m' = m_{s',t}$ if $b > 0$. To see that the second equation of Definition 7.1.7 will never be satisfied, we suppose for a contradiction that $m' = m_{s',t}$ and $m = m_{i',j}$ gives a solution to $p^a m' = m + r(p^f - 1)$ for $a > 0$ and $r > ep\left(\frac{p^a-1}{p-1}\right)$. Then

$$\begin{aligned} r = \frac{p^a m' - m}{p^f - 1} &\leqslant p^a\left(\frac{p-e}{p-1} + e - 1\right) - \frac{e}{p-1} \\ &= p^a\left(\frac{1}{p-1}\right) + e\left(\frac{p^{a+1} - 2p^a - 1}{p-1}\right). \end{aligned}$$

To find a contradiction we want to prove $r \leqslant ep\left(\frac{p^a-1}{p-1}\right)$. Simplifying the equations we find

$$\begin{aligned} p^a + e(p^{a+1} - 2p^a - 1) &\leqslant ep(p^a - 1) \\ \iff 0 &\leqslant p^a(2e-1) + e(1-p). \end{aligned}$$

However, the last inequality follows easily from $a \geqslant 1$:

$$p^a(2e-1) + e(1-p) \geqslant p(e-1) + e \geqslant 1$$

giving a contradiction, as required. $\square$

7.4.3.1. *Dependency graph.* Recall the definition of a dependency graph from §7.1.2.5. The typical pattern of dependencies in the generic case is captured in the graph of Figure 7.4.1

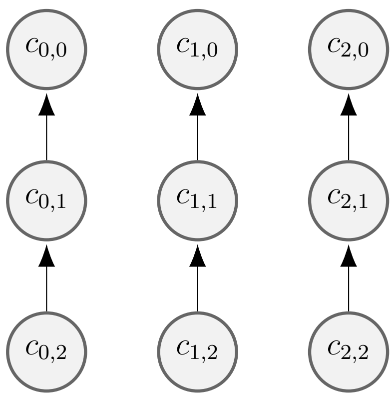

FIGURE 7.4.1. The dependency graph of any generic character χ assuming $f = 3$ and $e = 3$.

7.4.4. Conjectural formulae in the generic case. We will finish this section by giving a conjectural explicit formula for a spanning set of the spaces L_V^{AH} in terms of our basis elements $c_{i,j}$ in the generic case. Our set-up will be identical to the set-up at the beginning of Chapter 6. Fix a Serre weight $V = V_{\underline{\alpha},\underline{0}}$ and define the integers $r_i := \alpha_i + 1 \in [1, p]$. We recall that we defined integers $s_i, t_i \in [0, e-1] \cup [r_i, r_i+e-1]$ satisfying $t_i+s_i = r_i+e-1$, which correspond to the minimal and maximal Kisin modules of [GLS15]. For $i \in 0, \ldots, f-1$, we defined the intervals $\mathcal{I}_i := [0, s_i - 1]$ if $t_i \geqslant r_i$ and $\mathcal{I}_i := \{t_i\} \cup [r_i, s_i - 1]$ if $t_i < r_i$.

We would now like to define an f-tuple $(d_0, \ldots, d_{f-1})$ analogous to the set $\gamma(J)$ from §7.2 in which d_i should intuitively correspond to "the dimension at i". The easiest first definition to make is as follows.

Definition 7.4.5. We let $J := (\delta_0, \ldots, \delta_{f-1})$ be an f-tuple of non-negative integers which are defined by

$$\delta_i := |\mathcal{I}_i| = \begin{cases} s_i & \text{if } t_i \geqslant r_i, \\ s_i - r_i + 1 & \text{if } t_i < r_i, \end{cases}$$

for all $i \in 0, \ldots, f-1$. We note that $0 \leqslant \delta_i \leqslant e$ for all i.

As we saw already in §7.2, we need to apply a shift function γ before getting the correct dimensions. Let us define this function now.

Definition 7.4.6. We define a function $\gamma : \mathbf{Z}^f \to \mathbf{Z}^f$. Suppose we write $(y_0, \ldots, y_{f-1}) := \gamma(x_0, \ldots, x_{f-1})$. Then γ is defined by

$$y_i := \begin{cases} x_i & \text{if } t_i \geqslant r_i \text{ and } t_{i+1} \geqslant r_{i+1}, \\ x_i - 1 & \text{if } t_i < r_i \text{ and } t_{i+1} \geqslant r_{i+1}, \\ x_i + 1 & \text{if } t_i \geqslant r_i \text{ and } t_{i+1} < r_{i+1}, \\ x_i & \text{if } t_i < r_i \text{ and } t_{i+1} < r_{i+1}. \end{cases}$$

In other words, the function γ "shifts one dimension" from i to $i-1$ whenever $t_i < r_i$.

Definition 7.4.7. We let the f-tuple of integers $\gamma(J) := (d_0, \ldots, d_{f-1})$ be defined via $(d_0, \ldots, d_{f-1}) := \gamma(\delta_0, \ldots, \delta_{f-1})$. Note that we still have $0 \leqslant d_i \leqslant e$, since $\delta_i = e$ occurs only if $t_i < r_i$.

We may now state our conjecture regarding an explicit formula for $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ (see Definition 6.3.5) when χ is generic.

Conjecture 7.4.8. *Let $0 \leqslant i < f$ and $0 \leqslant j < e$. Suppose χ is generic and that the integers $m'_{i',j}$ and the function ϕ_j used in Definition 6.3.5 are explicitly defined as in Definition 7.4.2. Then*

$$(i, j) \in J_V^{\mathrm{AH}}(\chi_1, \chi_2) \text{ if and only if } j < d_i.$$

It follows from §7.4.3 that if the set $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ were to be defined according to the conjecture, then it would be admissible making it independent of the choice of the extension M and its uniformiser π used in the definition of the basis elements $u_{i,j}$ (as it would need to be). Ample computational evidence supports this conjecture.

We remark that it seems like a proof along the lines of §7.3.4 or [CEGM17, §3.6] is needed to prove the correctness of the conjecture – this amounts to proving some explicit combinatorial statement. If indeed this conjecture is proved, it should follow relatively easily from the results of this thesis that we get an extension of [DS15, Thm. B] to our more general notion of genericity.

7.5. Explicit formulae for $e = 2$

In the last section of this chapter, we will treat the special case when $e = 2$. As we will see, this case is some kind of "double layered" version of the case $e = 1$ from §7.2, where the basis elements $c_{0,0}, \ldots, c_{f-1,0}$ give the first "layer" and $c_{0,1}, \ldots, c_{f-1,1}$ the second. However, the interaction between the two layers means we see more complicated phenomena than in the unramified case alone. Mainly because of the increased difficulty of the underlying combinatorics, some arguments in this section remain conjectural. This case gives some indication of the potential complications involved in solving the explicit formula problem for $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ in general.

We assume K is an extension of $\mathbf{Q}_p$ of ramification degree 2, residue degree f and with a given fixed uniformiser π_K. As usual we fix a character $\chi : G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ and we write $(a_0, \ldots, a_{f-1})$ for the tame signature of χ. We will write f' for the absolute niveau of this character and we will assume for simplicity that $f = f'$ throughout this section – please see §5.1 for any unfamiliar definitions. We define $M := L(\pi)$ to be the extension of K obtained from an unramified extension L of K of degree prime-to-p and π a root of $x^{p^f-1} + \pi_K = 0$ such that $\chi|_{G_M}$ is trivial. When necessary we consider subscripts in $\mathbf{Z}/f\mathbf{Z}$ to lie in $\mathbf{Z}$, for example when considering a_j for some $j < i$ for a given i.

7.5.1. Explicit basis elements. Recall from §5.1 that we defined the integers n_i for $i \in 0, \dots, f-1$ via

$$n_i := \sum_{j=1}^{f} a_{i+j} p^{f-j} = a_{i+1} p^{f-1} + \cdots + a_{i-1} p + a_i.$$

For $0 \leqslant j < 2$ and $0 \leqslant i < f$, the integers $m_{i,j}$ were (non-explicitly) defined to be the integers $m \in \mathbf{Z}$ satisfying simultaneously

(1) $\frac{jp}{p-1} < \frac{m}{p^f-1} < \frac{(j+1)p}{p-1}$,
(2) $p \nmid m$ and
(3) there exists an i such that $m \equiv n_i \bmod p^f - 1$.

Denote the set of integers satisfying these three conditions by M_j. Our first goal is to find a natural explicit definition of the integers $m_{i,j}$ which behaves well under the dependencies of Definition 7.1.7.

Definition 7.5.1. Firstly, for the definition of $M_0 := \{m_{0,0}, \dots, m_{0,f-1}\}$ we apply the following two rules. For $0 \leqslant i < f$, we define

(1) if $a_i \neq p$, then we define $m_{i,0} := n_i$,
(2) if $a_i = p$, let s be the largest integer such that $s < i$ and $a_s \neq p-1$. Then we define $m_{i,0} := n_s - (p^f - 1)$.

Clearly, we now define the function $\phi_0 \colon \{0, \dots, f-1\} \to \{0, \dots, f-1\}$ via

$$\phi_0(i) := \begin{cases} i & \text{if } a_i \neq p; \\ s & \text{if } a_i = p. \end{cases}$$

It follows from the proof of Proposition 5.1.3 that this definition sets up a one-to-one correspondence between the set M_0 and $\{0, \dots, f-1\}$. The argument essentially follows from the idea that $n_s - (p^f - 1) > 0$ if and only if the coefficients of the top powers of p in n_s are equal to $(p-1, p-1, \dots, p-1, p, \dots)$ ordered from the highest to the lowest. The condition $p \nmid n_s - (p^f - 1)$ is equivalent to $a_s \neq p - 1$ meaning we have set up a one-to-one correspondence between $\{0 \leqslant i < f \mid a_i = p\}$ and elements of M_0 of the form $n_s - (p^f - 1)$. Together with the first equation of the definition, this sets up the required correspondence. We note that in the exceptional case that $(a_0, \dots, a_{f-1}) = (p-1, p-1, \dots, p-1, p)$ we include $s = i - f$ in our definition above.

Definition 7.5.2. Secondly, to define $M_1 := \{m_{0,1}, \dots, m_{f-1,1}\}$ we apply the following two rules. For $0 \leqslant i < f$, we define

(1) if $a_i \neq 1$, then we define $m_{i,1} := n_i + (p^f - 1)$,

(2) if $a_i = 1$, let s be the largest integer such that $s < i$ and $a_s \neq 2$. Then we define $m_{i,1} := n_s + 2(p^f - 1)$.

We define $\phi_1 \colon \{0, \dots, f-1\} \to \{0, \dots, f-1\}$ via

$$\phi_1(i) := \begin{cases} i & \text{if } a_i \neq 1; \\ s & \text{if } a_i = 1. \end{cases}$$

It follows from a very similar argument that this sets up a one-to-one correspondence between M_1 and $\{0, \dots, f-1\}$ with essentially the only difference being that we now note that $n_s + 2(p^f - 1) < 2p(p^f - 1)/(p-1)$ if and only if the top p powers of n_s are equal to $(2, 2, \dots, 2, 1, \dots)$ ordered from the highest to the lowest.

Remark 7.5.3. The two definitions above don't generalise well to beyond $e = 2$. One can use the proof of Proposition 5.1.3 to give an explicit definition of the integers $m_{i,j}$ for arbitrary e and f. However, defining these integers in this way makes the dependencies in the next subsection badly behaved (even for $e = 2$ already). It seems that the problem really boils down to finding canonical definitions of the integers $m_{i,j}$ in general, which is an issue the author does not, at present, know how to resolve.

7.5.2. Explicit dependencies. We will try to make the dependencies of Definition 7.1.8 explicit given the choice of the integers $m_{i,j}$ above. Since we have assumed throughout this section that $f' = f$, it suffices to check the two equations of Definition 7.1.7 to find all dependencies. We will give the explicit dependencies in the following propositions.

Proposition 7.5.4. *For all $0 \leqslant i < f$, we have that $(i, 1)$ depends on $(i, 0)$.*

Proof. If $a_i \neq 1, p$, then this follows straightforwardly since we have that $m_{i,1} = n_i + (p^f - 1) = m_{i,0} + (p^f - 1)$.

Suppose $a_i = p$ and s is the largest integer such that $s < i$ and $a_s \neq p-1$. Then $m_{i,0} = n_s - (p^f - 1)$ and $m_{i,1} = n_i + (p^f - 1)$. We claim that $n_i + (p^f - 1) = p^{i-s}(n_s - (p^f - 1)) + (p^f - 1)$. Indeed,

$$n_s - (p^f - 1) = a_{i+1}p^{f-(i-s+1)} + \cdots + a_s + 1$$

and $n_i = a_{i+1}p^{f-1} + \cdots + (a_s + 1)p^{i-s}$. Hence, $n_i - p^{i-s}(n_s - (p^f - 1)) = 0$ and the claim follows.

Suppose $a_i = 1$ and s is the largest integer such that $s < i$ and $a_s \neq 2$. Then $m_{i,0} = n_i$ and $m_{i,1} = n_s + 2(p^f - 1)$. We claim that

$$p^{i-s}(n_s + 2(p^f - 1)) = n_i + r(p^f - 1)$$

for some $r > 2p\left(\frac{p^{i-s}-1}{p-1}\right)$. Indeed, $n_s + 2(p^f - 1)$ equals

$$2p^f + 2p^{f-1} + \cdots + 2p^{f-(i-s)+1} + p^{f-(i-s)} + a_{i+1}p + \cdots + a_s - 2$$

and $n_i = a_{i+1}p^{f-1} + \cdots + a_s p^{i-s} + 2p^{i-s-1} + \cdots + 2p + 1$. So we find that

$$\begin{aligned} p^{i-s}(n_s + 2(p^f - 1)) - n_i &= (p^f - 1)(2p^{i-s} + 2p^{i-s-1} + \cdots + 2p + 1) \\ &> (p^f - 1)(2p^{i-s} + 2p^{i-s-1} + \cdots + 2p) \\ &= 2p\left(\frac{p^{i-s} - 1}{p - 1}\right)(p^f - 1), \end{aligned}$$

as required. □

Proposition 7.5.5. *Fix $0 \leqslant i < f$ such that $a_i = p$. Let s be the largest integer such that $s < i$ and $a_s \neq p - 1$. Then*

(1) for all $s < k < i$, we have that $(k, 0)$ and $(k, 1)$ depend on $(i, 0)$;
(2) if $a_s \neq p$, then $(s, 0)$ and $(s, 1)$ depend on $(i, 0)$;
(3) if $a_s = p$, then $(s, 1)$ and $(s - 1, 1)$ depend on $(i, 0)$.

Proof. We have that $m_{i,0} = n_s - (p^f - 1)$. Choose some integer k such that $s \leqslant k < i$ if $a_s \neq p$ and $s < k < i$ if $a_s = p$. For the first two parts of the proposition it suffices to prove that $(k, 0)$ depends on $(i, 0)$ by Proposition 7.5.4 and transitivity. In all these cases, we have $m_{k,0} = n_k$. We claim that $n_k = p^{k-s}(n_s - (p^f - 1)) + (p^f - 1)$. Indeed,

$$\begin{aligned} p^{k-s}(n_s - (p^f - 1)) &= p^{k-s}(a_{i+1}p^{f-(i-s)-1} + \cdots + a_s + 1) \\ &= a_{i+1}p^{f-(i-k)-1} + \cdots + (a_s + 1)p^{k-s}. \end{aligned}$$

Whereas

$$\begin{aligned} n_k = (p-1)p^{f-1} + \cdots + (p-1)p^{f-(i-k)+1} + p \cdot p^{f-(i-k)} + a_{i+1}p^{f-(i-k)-1} \\ + \cdots + a_s p^{k-s} + (p-1)p^{k-s-1} + \cdots + (p-1) \\ = p^f + a_{i+1}p^{f-(i-k)-1} + \cdots + (a_s + 1)p^{k-s} - 1, \end{aligned}$$

which proves the claim.

Suppose that $a_s = p$. We need to prove that $(s, 1)$ and $(s - 1, 1)$ depend on $(i, 0)$. The first claim follows instantly, since $m_{i,0} = n_s - (p^f - 1)$ and $m_{s,1} = n_s + (p^f - 1)$. For the second claim, we have two cases. Suppose first that $a_{s-1} \neq 1$. Then $m_{s-1,1} = n_{s-1} + (p^f - 1)$ and we claim that $pm_{s-1,1} = m_{i,0} + (2p + 1)(p^f - 1)$. This is easily seen as

$$p(n_{s-1} + (p^f - 1)) = n_s + (a_s + p)(p^f - 1) = n_s + 2p(p^f - 1).$$

If $a_{s-1} = 1$, then suppose s' is the largest integer such that $s' < s-1$ and $a_{s'} \neq 2$, so that $m_{s-1,1} = n_{s'} + 2(p^f - 1)$. We claim that

$$p^{s-s'} m_{s-1,1} = m_{i,0} + \left(2p\left(\frac{p^{s-s'}-1}{p-1}\right)+1\right)(p^f-1).$$

We see that

$$\begin{aligned} p^{s-s'} n_{s'} = 2p^{f+s-s'-1} + \cdots + 2p^{f+2} + p^{f+1} + pp^f \\ + a_{s+1}p^{f-1} + \cdots + a_{s'}p^{s-s'}. \end{aligned}$$

Hence, $p^{s-s'} n_{s'} - n_s = 2p\left(\frac{p^{s-s'-1}-1}{p-1}\right)(p^f-1)$. It follows straightforwardly that $p^{s-s'}(n_{s'} + 2(p^f-1)) - (n_s - (p^f-1))$ is equal to

$$\left(2p\left(\frac{p^{s-s'}-1}{p-1}\right)+1\right)(p^f-1),$$

as required. □

PROPOSITION 7.5.6. *Fix $0 \leqslant i < f$ and suppose $a_i = 1$. Let s be the largest integer such that $s < i$ and $a_s \neq 2$. Then*

(1) for all $s < k < i$, we have that $(i,1)$ depends on $(k,0)$ and on $(k,1)$;
(2) if $a_s \neq 1$, then $(i,1)$ depends on $(s,0)$ and on $(s,1)$;
(3) if $a_s = 1$, then $(i,1)$ depends on $(s,0)$ and on $(s-1,0)$.

PROOF. We note that $m_{i,1} = n_s + 2(p^f-1)$. We let k be an integer such that $s < k < i$. We note that it follows from transitivity and Proposition 7.5.4 that for the first part of the proposition it suffices to prove that $(i,1)$ depends on $(k,1)$, where $m_{k,1} = n_k + (p^f-1)$. We claim that

$$p^{k-s} m_{i,1} = m_{k,1} + \left(2p\left(\frac{p^{k-s}-1}{p-1}\right)+1\right)(p^f-1).$$

Similarly to before, we find that $p^{k-s}n_s - n_k = 2\left(\frac{p^{k-s}-1}{p-1}\right)(p^f-1)$. Again, it follows that $p^{k-s}(n_s + 2(p^f-1)) - (n_k + (p^f-1))$ equals

$$\left(2p\left(\frac{p^{k-s}-1}{p-1}\right)+1\right)(p^f-1).$$

If $a_s \neq 1$, then $m_{s,1} = n_s + (p^f-1)$. Since $m_{i,1} = n_s + 2(p^f-1)$, it follows instantly that $(i,1)$ depends on $(s,1)$. The dependence on $(s,0)$ follows from Proposition 7.5.4 and transitivity.

Lastly, suppose $a_s = 1$. Then we want to prove that $(i,1)$ depends on $(s,0)$ and on $(s-1,0)$. Since $m_{s,0} = n_s$, the first claim is automatic. For the second claim we have two cases. First assume that $a_{s-1} \neq p$. Then we claim that $m_{i,1} = pm_{s-1,0} + (p^f-1)$. Indeed, we see that $pn_{s-1} - n_s = (p^f-1)$, so the claim follows easily as $m_{s-1,0} = n_{s-1}$ and $m_{i,1} = n_s + 2(p^f - 1)$. Now assume that $a_{s-1} = p$ and let s' be the largest integer such that $s' < s - 1$ and $a_{s'} \neq p - 1$. We claim that $m_{i,1} = p^{s-s'} m_{s-1,0} + (p^f - 1)$. Similarly to before, $p^{s-s'} n_{s'} = n_s + (p^{s-s'} + 1)(p^f - 1)$, and the claim follows easily since $m_{s-1,0} = n_{s'} - (p^f - 1)$. □

CONJECTURE 7.5.7. *For $e = 2$ and with the explicit choice of the integers $m_{i,j}$ from §7.5.1, the three propositions above give all possible dependencies of Definition 7.1.8.*

We note that in the case that χ is generic neither Proposition 7.5.5 nor Proposition 7.5.6 applies so that only the dependencies of Proposition 7.5.4 remain.

The conjecture is supported by strong computational evidence. A possible proof of the conjecture will be a more complicated version of the proof of Proposition 7.2.3 and we have only attempted a proof briefly. This is mainly because a potential explicit formula for $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ when $e = 2$ and a proof of the correctness of this formula would render the need of the equivalence of the two definitions of dependence unnecessary through Corollary 6.3.10. Nonetheless, the explicit dependencies given here are useful for finding an explicit formula in the next subsection.

7.5.2.1. *Dependency graphs.* Recall the notion of a dependency graph from §7.1.2.5. In the case of $e = 2$ we have a number of different possible prototypical examples of a dependency graph. Figures 7.5.1 and 7.5.2 cover the two special cases of Proposition 7.5.5 and Figures 7.5.3 and 7.5.4 cover the two special cases of Proposition 7.5.6. Therefore, the dependency graph of a general character χ can be obtained as an appropriate combination of these figures. We have assumed $p > 3$ in these figures.

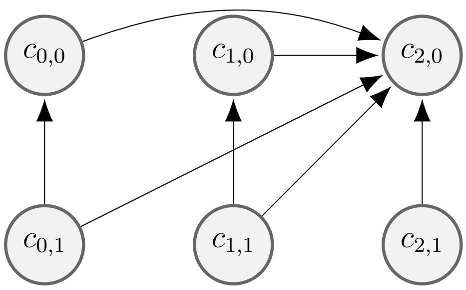

FIGURE 7.5.1. The dependency graph of a character χ with tame signature $(a_0, p - 1, p)$ for any $1 < a_0 < p - 1$ assuming $e = 2$.

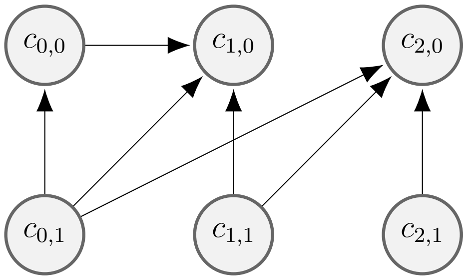

FIGURE 7.5.2. The dependency graph of a character χ with tame signature (a_0, p, p) for any $1 < a_0 < p-1$ assuming $e = 2$.

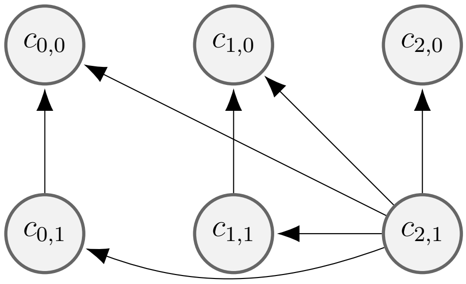

FIGURE 7.5.3. The dependency graph of a character χ with tame signature $(a_0, 2, 1)$ for any $2 < a_0 < p$ assuming $e = 2$.

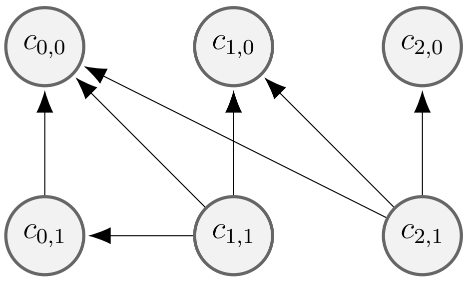

FIGURE 7.5.4. The dependency graph of a character χ with tame signature $(a_0, 1, 1)$ for any $2 < a_0 < p$ assuming $e = 2$.

7.5.3. Shift functions for $e = 2$. In this subsection we will give explicit shift functions allowing us to conjecture an alternative explicit version of $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ when $e = 2$. It will be clear to the reader familiar with the paper [DDR16] that the approach here is loosely based on their §7.1. However, the situation for $e = 2$ is already substantially more complicated than the unramified case and we will need to make the necessary adjustments along the way.

Initially our set-up will be very similar to the generic case of §7.4. We start with a reducible representation $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbf{F}}_p)$ of the form

$$\rho \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}.$$

Fix a Serre weight $V = V_{\underline{\alpha},\underline{0}}$ and the integers $r_i := \alpha_i + 1 \in [1, p]$. We recall that we defined integers $s_i, t_i \in [0, 1] \cup [r_i, r_i + 1]$ satisfying $t_i + s_i = r_i + 1$, which correspond to the minimal and maximal Kisin modules of [GLS15]. For $i \in 0, \ldots, f - 1$, we defined the intervals $\mathcal{I}_i := [0, s_i - 1]$ if $t_i \geqslant r_i$ and $\mathcal{I}_i := \{t_i\} \cup [r_i, s_i - 1]$ if $t_i < r_i$.

Our goal is to define an f-tuple $(d_0, \ldots, d_{f-1})$ in which the integer $0 \leqslant d_i \leqslant 2$ represents the 'dimension at i', or, said differently, in generic cases d_i should be the number of elements of the set $\{(i, 0), (i, 1)\}$ included in $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$.

Definition 7.5.8. We let $J := (\delta_0, \ldots, \delta_{f-1})$ be an f-tuple of non-negative integers which are defined by

$$\delta_i := |\mathcal{I}_i| = \begin{cases} s_i & \text{if } t_i \geqslant r_i, \\ s_i - r_i + 1 & \text{if } t_i < r_i, \end{cases}$$

for all $i \in 0, \ldots, f - 1$. We note that $0 \leqslant \delta_i \leqslant 2$ for all i.

As in the generic case of §7.4 we need to apply a shift function. Recall the definition of the shift function γ in Definition 7.4.6.

Definition 7.5.9. We define the f-tuple $\gamma(J) := (d_0, \ldots, d_{f-1})$ via $(d_0, \ldots, d_{f-1}) := \gamma(\delta_0, \ldots, \delta_{f-1})$. We observe that we still have $0 \leqslant d_i \leqslant 2$.

7.5.3.1. *The shift function μ.* Unlike the generic case, we need to define a shift function μ analogous to the shift function μ we saw in the unramified case in §7.2.3.1. The issue at hand is that we know (as long as we believe our conjectures) that the spaces L_V^{AH} are independent of the choices of π_K, π and L. Therefore, we expect any explicit formula for $J_V^{\mathrm{AH}}(\chi_1, \chi_2)$ to satisfy the admissibility condition of Definition 7.1.12. However, in non-generic cases simply defining

$$\{(i, j) \in \mathbf{Z}/f\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z} \mid j < d_i\}$$

often gives terribly non-admissible sets. That is why another shift function μ is needed.

Our shift function μ is similar to the shift function μ from §7.2.3.1. First we define two functions $\theta_0, \theta_1 : \mathbf{Z} \to \mathbf{Z}$ as follows: for any $j \in \mathbf{Z}$ let

$$\theta_0(j) := \begin{cases} i & \text{if } (a_j, p-1, \ldots, p-1, \underset{\substack{\| \\ a_i}}{p}) \text{ for } i > j, \\ j & \text{otherwise.} \end{cases}$$

We note that here there are no restrictions of the value of a_j. We allow for $a_i = p$ and $j = i - 1$ and we include the case that $i = j + f$ if $\underline{a} = (p, p-1, \ldots, p-1)$. Similarly for any $j \in \mathbf{Z}$ we define

$$\theta_1(j) := \begin{cases} i & \text{if } (a_j, 2, \ldots, 2, \underset{\substack{\| \\ a_i}}{1}) \text{ for } i > j, \\ j & \text{otherwise.} \end{cases}$$

Obviously, our functions θ_0, θ_1 induce functions $\mathbf{Z}/f\mathbf{Z} \to \mathbf{Z}/f\mathbf{Z}$ which we will denote by the same name.

Now we are ready to define our function μ. Our definition of μ comes in two parts: the part μ_0 for dealing with the dependencies of Proposition 7.5.5 and the part μ_1 for dealing with the dependencies of Proposition 7.5.6. Let us do the former first.

Fix any f-tuple $J' := (x_0, \ldots, x_{f-1})$ satisfying $0 \leqslant x_i \leqslant 2$. Recursively, we will redefine J' and the final recursion will give $\mu_0(J')$. We define

$$\mathcal{P}_{J'} := \{i \in \mathbf{Z}/f\mathbf{Z} \mid x_i > 0\}$$

to be the subset of indices where we have a positive dimension. If we have that $\theta_0(\mathcal{P}_{J'}) \subseteq \mathcal{P}_{J'}$, then we let $\mu_0(J') = J'$. Otherwise we pick any $[i_0] \in \theta_0(\mathcal{P}_{J'}) \backslash \mathcal{P}_{J'}$. Suppose j_0 is the largest integer such that $j_0 < i_0$, $[j_0] \in \mathcal{P}_{J'}$ and $\theta_0(j_0) = i_0$. Then we define $J'_0 := (x_{0,0}, \ldots, x_{0,f-1})$, our first recursion, via

$$x_{0,k} := \begin{cases} x_{j_0} - 1 & \text{if } k = j_0; \\ 1 = x_{i_0} + 1 & \text{if } k = i_0; \\ x_k & \text{otherwise,} \end{cases}$$

for $k \in \{0, \ldots, f-1\}$. For the remaining recursions, we list representatives of all classes of $\mathbf{Z}/f\mathbf{Z}$ in decreasing order starting at j_0 and denote them by $j_0 > j_1 > j_2 > \ldots > j_{f-1} > j_0 - f$. For $\kappa \in \{1, \ldots, f-1\}$, we recursively define $J'_\kappa := (x_{\kappa,0}, \ldots, x_{\kappa,f-1})$ via $J'_\kappa = J'_{\kappa-1}$ unless $j_\kappa \in \mathcal{P}_{J'}$ and $x_{\kappa-1,\theta_0(j_\kappa)} = 0$

in which case we define

$$x_{\kappa,k} := \begin{cases} x_{\kappa-1,j_\kappa} - 1 & \text{if } k = j_\kappa; \\ 1 = x_{\kappa-1,\theta_0(j_\kappa)} + 1 & \text{if } k = \theta_0(j_\kappa); \\ x_{\kappa-1,k} & \text{otherwise,} \end{cases}$$

for $k \in \{0, \ldots, f-1\}$. We define $\mu_0(J') := J'_{f-1}$.

We can define μ_1 analogously by carefully keeping track of the correct 'dual' analogue of the previous case. We start with any $J' := (x_0, \ldots, x_{f-1})$ satisfying $0 \leqslant x_i \leqslant 2$. We define

$$\mathcal{S}_{J'} := \{i \in \mathbf{Z}/f\mathbf{Z} \mid x_i < 2\}$$

to be the subset of indices where we have a dimension that is not full. If $\theta_1(\mathcal{S}_{J'}) \subseteq \mathcal{S}_{J'}$, then we let $\mu_1(J') = J'$. Otherwise we pick any class $[i_0] \in \theta_1(\mathcal{S}_{J'})\backslash\mathcal{S}_{J'}$. Suppose j_0 is the largest integer such that $j_0 < i_0$, $[j_0] \in \mathcal{S}_{J'}$ and $\theta_1(j_0) = i_0$. Then we define $J'_0 := (x_{0,0}, \ldots, x_{0,f-1})$, our first recursion, via

$$x_{0,k} := \begin{cases} x_{j_0} + 1 & \text{if } k = j_0; \\ 1 = x_{i_0} - 1 & \text{if } k = i_0; \\ x_k & \text{otherwise,} \end{cases}$$

for $k \in \{0, \ldots, f-1\}$. For the remaining recursions we list representatives of all classes of $\mathbf{Z}/f\mathbf{Z}$ in decreasing order starting at j_0 and denote them by $j_0 > j_1 > j_2 > \ldots > j_{f-1} > j_0 - f$. For $\kappa \in \{1, \ldots, f-1\}$, we recursively define $J'_\kappa := (x_{\kappa,0}, \ldots, x_{\kappa,f-1})$ via $J'_\kappa = J'_{\kappa-1}$ unless $j_\kappa \in \mathcal{S}_{J'}$ and $x_{\kappa-1,\theta_1(j_\kappa)} = 2$ in which case we define

$$x_{\kappa,k} := \begin{cases} x_{\kappa-1,j_\kappa} + 1 & \text{if } k = j_\kappa; \\ 1 = x_{\kappa-1,\theta_1(j_\kappa)} - 1 & \text{if } k = \theta_1(j_\kappa); \\ x_{\kappa-1,k} & \text{otherwise,} \end{cases}$$

for $k \in \{0, \ldots, f-1\}$. We define $\mu_1(J') := J'_{f-1}$. Now we define

$$\mu(J') := \mu_1 \circ \mu_0(J').$$

Since μ is defined as the repeated application of certain shift-functions, it is clear from the definition that $\mu(J')$ has the same *degree* as J', where we define the degree of an f-tuple $(x_0, \ldots, x_{f-1})$ as

$$\deg(x_0, \ldots, x_{f-1}) := \sum_{i=0}^{f-1} x_i.$$

We will use the notation $\mu(J') = (\mu(x_0), \ldots, \mu(x_{f-1}))$, i.e. we denote the ith entry of the f-tuple $\mu(J')$ by $\mu(x_i)$.

PROPOSITION 7.5.10. *The shift functions μ_0 and μ_1 are independent of the choices in their definitions.*

PROOF. Let $(a_0, \ldots, a_{f-1})$ be any tame signature (i.e. $1 \leqslant a_i \leqslant p$ and $a_i < p$ for at least one i) and $J' := (x_0, \ldots, x_{f-1})$ is some index of dimensions (i.e. $0 \leqslant x_i \leqslant 2$ for all i).

Suppose first that i_0, i_0' are integers such that $[i_0], [i_0'] \in \theta_0(\mathcal{P}_{J'})\backslash\mathcal{P}_{J'}$. We assume without loss of generality that $i_0 < i_0'$ and $i_0, i_0' \in [0, f-1]$. Let j_0 (resp. j_0') be the largest integer such that $j_0 < i_0$ (resp. $j_0' < i_0'$), $\theta_0(j_0) = i_0$ (resp. $\theta_0(j_0') = i_0'$) and $[j_0] \in \mathcal{P}_{J'}$ (resp. $[j_0'] \in \mathcal{P}_{J'}$). It follows from the definition of θ_0 that $i_0 \leqslant j_0'$ as $a_{i_0} = p$. But since $[i_0] \notin \mathcal{P}_{J'}$ and $[j_0'] \in \mathcal{P}_{J'}$, we see that $i_0 < j_0'$. Independence of choice now follows easily by chasing through the definitions when starting at i_0 and i_0' and noticing that you end up with the same set $\mu_0(J')$ in either case. The argument for μ_1 is similar. $\square$

LEMMA 7.5.11. *Suppose Conjecture 7.5.7 is true. Let $(a_0, \ldots, a_{f-1})$ be any tame signature (i.e. $1 \leqslant a_i \leqslant p$ and $a_i < p$ for at least one i) and $J' := (x_0, \ldots, x_{f-1})$ is some index of dimensions (i.e. $0 \leqslant x_i \leqslant 2$ for all i). Then the set defined by*

$$\{(i,j) \in \mathbf{Z}/f\mathbf{Z} \times \mathbf{Z}/e\mathbf{Z} \mid j < \mu(d_i)\}$$

is admissible in the sense of Definition 7.1.12.

Under the assumption of Conjecture 7.5.7 this lemma follows essentially from unravelling the definition of μ using the explicit dependencies of the previous subsection. It is similar to Lemma 7.1 of [DDR16]. We will not give a proof here, because independence of the choices follows immediately from Corollary 6.3.10 once the conjecture below is proved.

CONJECTURE 7.5.12. *For $e = 2$, J and $\mu(\gamma(J)) := (\mu(d_0), \ldots, \mu(d_{f-1}))$ be as above. Suppose that the integers $m'_{i',j}$ and the functions ϕ_0, ϕ_1 used in Definition 6.3.5 are explicitly defined as in Definitions 7.5.1 and 7.5.2. Then, for $0 \leqslant i < f$ and $0 \leqslant j < e$, we have that*

$$(i,j) \in J_V^{\mathrm{AH}}(\chi_1, \chi_2) \textit{ if and only if } j < \mu(d_i).$$

We have collected strong computational evidence for this conjecture. Again, it is a proof of an explicit combinatorial statement that is needed along the lines of §3.6 of [CEGM17] in the unramified case or §7.3.4 in the totally ramified case.

REMARK 7.5.13. We remark that, in general, $\mu_0 \circ \mu_1 \neq \mu_1 \circ \mu_0$. For example, if $p = 5, e = 2, f = 3$ and the tame signature $(a_0, a_1, a_2) = (1, 1, 5)$. We have that $r = (2, 4, 2)$, $t = (3, 4, 1)$ and $s = (0, 1, 2)$ give $\gamma(J) = (0, 2, 0)$. Therefore, we see that $\mu_1 \circ \mu_0(\gamma(J)) = (0, 1, 1)$. On the other hand, we find that $\mu_0 \circ \mu_1(\gamma(J)) = (1, 0, 1)$. Only the first gives the correct basis elements. In other words, the order matters in the definition of μ.

Index

Bibliography

[Abr89] Victor Abrashkin. “Modular representations of the Galois group of a local field and a generalization of a conjecture of Shafarevich”. In: *Izv. Akad. Nauk SSSR Ser. Mat.* 53.6 (1989), pp. 1135–1182.

[Abr97] Victor Abrashkin. “The field of norms functor and the Brückner–Vostokov formula”. In: *Math. Ann.* 308.1 (1997), pp. 5–19.

[AS86a] Avner Ash and Glenn Stevens. “Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues.” In: *J. Reine. Angew. Math.* 365 (1986), pp. 192–220.

[AS86b] Avner Ash and Glenn Stevens. “Modular forms in characteristic ℓ and special values of their L -functions”. In: *Duke Math. J.* 53.3 (1986), pp. 849–868.

[BC09] Olivier Brinon and Brian Conrad. *CMI Summer School Notes on p-adic Hodge Theory.* June 2009. Retrieved on 16 Aug 2019 from `http://math.stanford.edu/~conrad/papers/notes.pdf`.

[BDJ10] Kevin Buzzard, Fred Diamond, and Frazer Jarvis. “On Serre's conjecture for mod ℓ Galois representations over totally real fields”. In: *Duke Math. J.* 155.1 (2010), pp. 105–161.

[Ber04] Laurent Berger. “An introduction to the theory of p-adic representations”. In: *Geometric aspects of Dwork theory.* Vol. 1. de Gruyter, 2004, pp. 255–292.

[BL94] Laure Barthel and Ron Livné. “Irreducible modular representations of GL_2 of a local field”. In: *Duke Math. J.* 75.2 (1994), pp. 261–292.

[Bla05] Régis Blache. “A Stickelberger theorem for p-adic Gauss sums”. In: *Acta Arithmetica* 118.1 (2005), pp. 11–26.

[BLGG13] Thomas Barnet-Lamb, Toby Gee, and David Geraghty. “Serre weights for rank two unitary groups”. In: *Mathematische Annalen* 356.4 (2013), pp. 1551–1598.

[Bre00] Christophe Breuil. "Groupes p-Divisibles, Groupes Finis et Modules Filtrés". In: *Ann. of Math.* 152.2 (2000), pp. 489–549.

[CEGM17] Frank Calegari, Matthew Emerton, Toby Gee, and Lambros Mavrides. "Explicit Serre weights for two-dimensional Galois representations". In: *Compositio Mathematica* 153.9 (2017), pp. 1893–1907.

[CEGS19] Ana Caraiani, Matthew Emerton, Toby Gee, and David Savitt. "Moduli stacks of two-dimensional Galois representations". (Preprint). 2019. URL: https://arxiv.org/abs/1908.07019.

[CH18] Jean-Luc Chabert and Emmanuel Halberstadt. "On Abhyankar's lemma about ramification indices". (Preprint). 2018. URL: https://arxiv.org/abs/1805.08869.

[DDR16] Lassina Dembélé, Fred Diamond, and David P. Roberts. "Serre weights and wild ramification in two-dimensional Galois representations". In: *Forum of Mathematics, Sigma* 4 (2016), e33.

[Del71] Pierre Deligne. "Formes modulaires et représentations l-adiques". In: *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*. Vol. 175. Lecture Notes in Math. Springer, Berlin, 1971, Exp. No. 355, pp. 139–172.

[DI95] Fred Diamond and Jongpil Jeong Illkyun Im. "Modular forms and modular curves". In: *Seminar on Fermat's last theorem.* CMS Conference Proceedings. American Math. Soc., 1995.

[DS15] Fred Diamond and David Savitt. "Serre weights for locally reducible two-dimensional Galois representations." In: *J. Inst. Math. Jussieu* 14.3 (2015), pp. 639–672.

[DV13] Lassina Dembélé and John Voight. "Explicit Methods for Hilbert Modular Forms". In: *Elliptic Curves, Hilbert Modular Forms and Galois Deformations*. Springer, 2013, pp. 135–198.

[Edi92] Bas Edixhoven. "The weight in Serre's conjectures on modular forms". In: *Invent. math.* 109.3 (1992), pp. 563–594.

[Fal87] Gerd Faltings. "Hodge-tate structures and modular forms". In: *Mathematische Annalen* 278.1 (1987), pp. 133–149.

[FJ95] Gerd Faltings and Bruce W. Jordan. "Crystalline cohomology and $\mathrm{GL}(2, \mathbf{Q})$". In: *Israel J. Math.* 90.1 (1995), pp. 1–66.

[Fon85] Jean-Marc Fontaine. "Il n'y a pas de variété abélienne sur $\mathbf{Z}$." In: *Invent. math.* 81 (1985), pp. 515–538.

[Fre90] Eberhard Freitag. *Hilbert modular forms*. Springer-Verlag, 1990.

[Gar89] Paul B. Garrett. *Holomorphic Hilbert Modular Forms*. Taylor & Francis, 1989.

[Gee11] Toby Gee. “Automorphic lifts of prescribed types”. In: *Mathematische Annalen* 350.1 (2011), pp. 107–144.

[GHS18] Toby Gee, Florian Herzig, and David L Savitt. “General Serre weight conjectures”. In: *Journal of the European Mathematical Society* 20.12 (2018), pp. 2859–2949.

[GLS12] Toby Gee, Tong Liu, and David Savitt. “Crystalline extensions and the weight part of Serre’s conjecture”. In: *Algebra and Number Theory* 6.7 (2012), pp. 1537–1559.

[GLS15] Toby Gee, Tong Liu, and David Savitt. “The weight part of Serre’s conjecture for GL(2)”. In: *Forum of Mathematics, Pi* 3 (2015).

[GS04] Alexandre Grothendieck and Jean-Pierre Serre. *Grothendieck-Serre correspondence*. Ed. by Pierre Colmez and Jean-Pierre Serre. Bilingual ed. Providence, R.I. : American Mathematical Society, 2004.

[Her10] Florian Herzig. *Explicit Serre Weight Conjectures*. Oct. 2010. Retrieved on 16 Aug 2019 from `https://video.ias.edu/file/37715`.

[Jar97] Frazer Jarvis. “On Galois representations associated to Hilbert modular forms”. In: *J. Reine Angew. Math.* 491 (1997), pp. 199–216.

[Kis06] Mark Kisin. “Crystalline representations and F-crystals”. In: *Algebraic Geometry and Number Theory*. Birkhäuser Boston, 2006, pp. 459–496.

[Kra11] Darci L. Kracht. “Applications of the Artin–Hasse exponential series and its generalisations to finite algebra groups”. PhD thesis. Kent State University, 2011.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. “Serre’s modularity conjecture (I)”. In: *Inventiones mathematicae* 178.3 (2009), pp. 485–504.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. “Serre’s modularity conjecture (II)”. In: *Inventiones mathematicae* 178.3 (2009), pp. 505–586.

[Mul13] Alain Muller. “Relèvements cristallins de représentations galoisiennes”. PhD thesis. Université de Strasbourg, 2013.

[Rob00] Alain M. Robert. *A Course in p-adic Analysis.* Graduate Texts in Mathematics. Springer, 2000.

[RS01] Kenneth A. Ribet and William A. Stein. "Lectures on Serre's conjectures". In: *Arithmetic algebraic geometry.* Ed. by Karl Rubin and Brian Conrad. Providence, RI: American Mathematical Society (AMS), 2001, pp. 143–232.

[SageMath] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.1).* `https://www.sagemath.org`. 2017.

[Sch08] Michael M. Schein. "Weights in Serre's conjecture for Hilbert modular forms: The ramified case". In: *Israel Journal of Mathematics* 166.1 (2008), pp. 369–391.

[Sch13] Michael M. Schein. "Serre's modularity conjecture". In: *Travaux Math.* 23 (2013), pp. 139–172.

[Ser79] Jean-Pierre Serre. *Local Fields.* English Edition (translated by Marvin Jay Greenberg). Graduate Texts in Mathematics. Springer, 1979.

[Ser87] Jean-Pierre Serre. "Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)". In: *Duke Math. J.* 54.1 (1987), pp. 179–230.

[ST15] Pierre Colmez and Jean–Pierre Serre, eds. *Correspondance Serre–Tate.* Documents Mathematiques. Société Mathématique de France, 2015.

[Wan17] Xiyuan Wang. "Weight elimination in two dimensions when $p = 2$". (Preprint). 2017. URL: `https://arxiv.org/abs/1711.09035`.